

# Wi-Fi Protected Access (WPA) in een configuratievoorbeeld van Cisco Unified Wireless Network

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Ondersteuning van WPA en WPA2](#)

[Netwerkinstelling](#)

[De apparaten voor WPA2 Enterprise Mode configureren](#)

[Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server](#)

[Configureer de WLAN voor WPA2 Enterprise Mode](#)

[De RADIUS-server voor WPA2 Enterprise Mode-verificatie configureren \(EAP-FAST\)](#)

[De draadloze client voor WPA2 Enterprise Mode configureren](#)

[De apparaten configureren voor WPA2 Personal Mode](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u Wi-Fi Protected Access (WPA) kunt configureren in een Cisco Unified Wireless Network.

## Voorwaarden

### Vereisten

Zorg ervoor dat u basiskennis van deze onderwerpen hebt voordat u deze configuratie probeert:

- WPA
- Draadloze LAN (WLAN)-beveiligingsoplossingen **N.B.:** Raadpleeg [Cisco Wireless LAN Security - Overzicht](#) voor informatie over Cisco WLAN-beveiligingsoplossingen.

### Gebruikte componenten

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

- Cisco 1000 Series lichtgewicht access point (LAP)
- Cisco 4404 draadloze LAN-controller (WLC) waarop firmware 4.2.61.0 wordt uitgevoerd
- Cisco 802.11a/b/g-clientadapter waarop firmware 4.1 wordt uitgevoerd
- Aironet Desktop Utility (ADU) werkt met firmware 4.1
- Cisco Secure ACS-server versie 4.1

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.

## Ondersteuning van WPA en WPA2

Het Cisco Unified Wireless Network biedt ondersteuning voor de Wi-Fi Alliance-certificeringen WPA en WPA2. WPA is geïntroduceerd door de Wi-Fi Alliance in 2003. WPA2 werd geïntroduceerd door de Wi-Fi Alliance in 2004. Alle producten die Wi-Fi-gecertificeerd zijn voor WPA2 moeten compatibel zijn met producten die Wi-Fi-gecertificeerd zijn voor WPA.

WPA en WPA2 bieden een hoge mate van zekerheid voor eindgebruikers en netwerkbeheerders dat hun gegevens privé zullen blijven en dat de toegang tot hun netwerken wordt beperkt tot geautoriseerde gebruikers. Beide hebben persoonlijke en bedrijfsmodi die voldoen aan de specifieke behoeften van de twee marktsegmenten. In de Enterprise-modus van elk programma worden IEEE 802.1X en EAP gebruikt voor verificatie. De persoonlijke modus van elk gebruik van Pre-Shared Key (PSK) voor verificatie. Cisco raadt geen Personal Mode aan voor bedrijfs- of overheidimplementaties, omdat het een PSK gebruikt voor gebruikersverificatie. PSK is niet veilig voor ondernemingsmilieu's.

Met WPA worden alle bekende WEP-kwetsbaarheden in de oorspronkelijke IEEE 802.11-beveiligingsimplementatie aangepakt en wordt een onmiddellijke beveiligingsoplossing voor WLAN's in zowel ondernemingen als in SOHO-omgevingen (Small Office/Home Office) geïntroduceerd. WPA maakt gebruik van TKIP voor de codering.

WPA2 is de volgende generatie van Wi-Fi-beveiliging. Het is de interoperabele implementatie van de Wi-Fi Alliance van de geratificeerde IEEE 802.11i norm. Het implementeert het door het National Institute of Standards and Technology (NIST) aanbevolen AES-encryptie-algoritme met behulp van Counter Mode met Cycle Block Chaining Message Authenticatie Code Protocol (CCMP). WPA2 vergemakkelijkt de naleving van FIPS 140-2 van de overheid.

### Vergelijking van WPA- en WPA2-modemtypen

	WPA	WPA2
<b>Enterprise Mode (Bedrijf, Overheid, Onderwijs)</b>	<ul style="list-style-type: none"> <li>• Verificatie: IEEE 802.1X/EA P</li> <li>• Encryptie: TKIP/MIC</li> </ul>	<ul style="list-style-type: none"> <li>• Verificatie: IEEE 802.1X/EA P</li> <li>• Versleuteli ng: AES-</li> </ul>

		CCMP
<b>Persoonlijke modus (SOHO, Thuis/Persoonlijk)</b>	<ul style="list-style-type: none"> <li>• Verificatie: PSK</li> <li>• Encryptie: TKIP/MIC</li> </ul>	<ul style="list-style-type: none"> <li>• Verificatie: PSK</li> <li>• Versleuteling: AES-CCMP</li> </ul>

In de Enterprise-modus gebruiken zowel WPA als WPA2 802.1X/EAP voor verificatie. 802.1X biedt WLAN's met sterke wederzijdse verificatie tussen een client en een verificatieserver. Daarnaast biedt 802.1X dynamische coderings sleutels per gebruiker, per sessie, waardoor de administratieve belasting en beveiligingsproblemen met betrekking tot statische coderings sleutels worden verwijderd.

Met 802.1X worden de aanmeldingsgegevens die voor de verificatie worden gebruikt, zoals aanmeldingswachtwoorden, nooit op het draadloze medium verzonden, of zonder encryptie. Terwijl 802.1X-verificatietypen zorgen voor sterke verificatie voor draadloze LAN's, zijn TKIP of AES nodig voor codering, naast 802.1X-codering omdat de standaard 802.11 WEP-codering kwetsbaar is voor netwerkaanvallen.

Er bestaan verschillende 802.1X-verificatietypen, die elk een andere benadering van verificatie bieden en tegelijkertijd vertrouwen op hetzelfde framework en EAP voor communicatie tussen een client en een toegangspunt. Cisco Aironet-producten ondersteunen meer 802.1X EAP-verificatietypen dan andere WLAN-producten. Ondersteunde typen zijn onder meer:

- [Cisco LEAP](#)
- [EAP-Flexibele verificatie via beveiligde tunneling \(EAP-FAST\)](#)
- EAP-Transport Layer Security (EAP-TLS)
- [Protected Extensible Verification Protocol \(PEAP\)](#)
- EAP-Tunneling (EAP-TTLS)
- EAP-Subscriber Identity Module (EAP-SIM)

Een ander voordeel van 802.1X-verificatie is gecentraliseerd beheer voor WLAN-gebruikersgroepen, inclusief op beleid gebaseerde sleutelrotatie, dynamische sleuteltoewijzing, dynamische VLAN-toewijzing en SSID-bepalking. Deze functies roteren de coderingstoetsen.

In de persoonlijke werkwijze wordt een vooraf gedeelde sleutel (wachtwoord) gebruikt voor verificatie. Voor de persoonlijke modus zijn alleen een toegangspunt en clientapparaat nodig, terwijl voor de Enterprise-modus doorgaans een RADIUS of andere verificatieserver op het netwerk nodig is.

Dit document bevat voorbeelden voor het configureren van WPA2 (Enterprise-modus) en WPA2-PSK (Persoonlijke modus) in een Cisco Unified Wireless-netwerk.

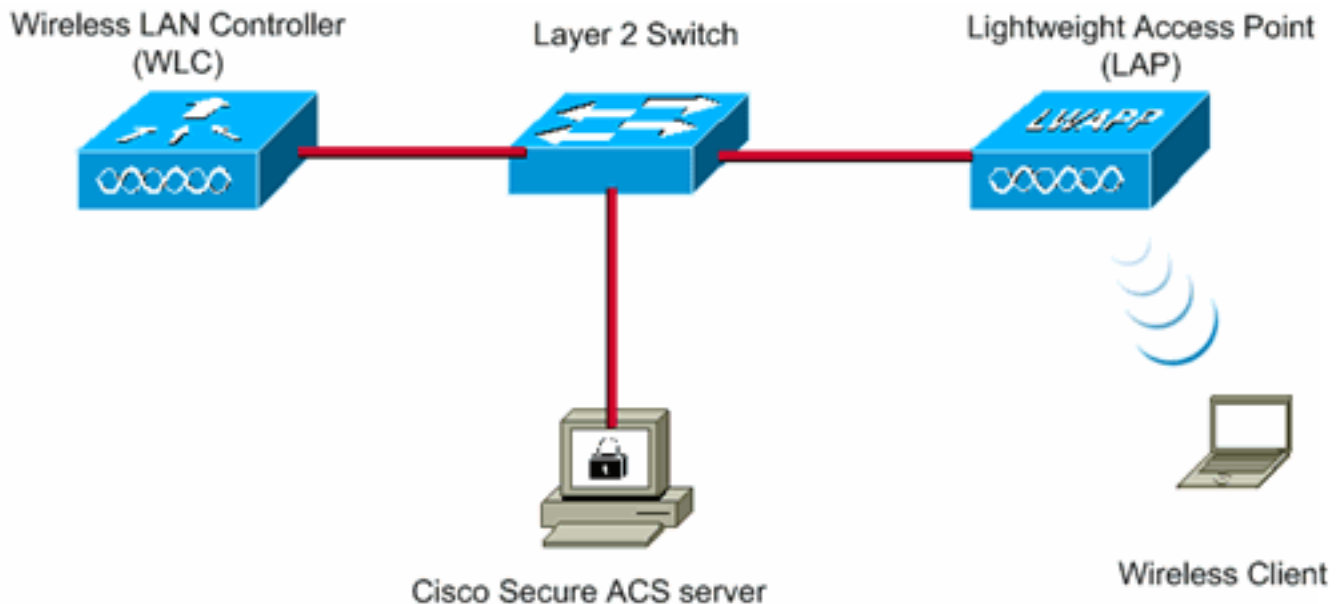
## [Netwerkinstelling](#)

In deze installatie worden een Cisco 4404 WLC en een Cisco 1000 Series LAP aangesloten via een Layer 2-Switch. Een externe RADIUS-server (Cisco Secure ACS) is ook verbonden met dezelfde switch. Alle apparaten bevinden zich in hetzelfde subnetje. Het toegangspunt (LAP) is aanvankelijk geregistreerd bij de controller. Er moeten twee draadloze LAN's worden gemaakt, één voor de WPA2 Enterprise-modus en één voor de WPA2 Personal-modus.

WPA2-Enterprise mode WLAN (SSID: WPA2-Enterprise) gebruikt EAP-FAST voor het verifiëren van de draadloze clients en AES voor codering. Cisco Secure ACS-server wordt gebruikt als de externe RADIUS-server voor verificatie van de draadloze clients.

WPA2-Personal mode WLAN (SSID: WPA2-PSK) gebruikt WPA2-PSK voor de verificatie met de vooraf gedeelde sleutel "backdefghijk".

U dient de apparaten voor deze installatie te configureren:



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

## [De apparaten voor WPA2 Enterprise Mode configureren](#)

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

Voer deze stappen uit om de apparaten te configureren voor de werkmodus WPA2 Enterprise:

1. [Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server](#)
2. [Het WLAN configureren voor WPA2 Enterprise Mode Verification \(EAP-FAST\)](#)
3. [De draadloze client voor WPA2 Enterprise Mode configureren](#)

### [Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server](#)

De WLC moet worden geconfigureerd om de gebruikersreferenties te kunnen doorsturen naar een externe RADIUS-server. De externe RADIUS-server valideert vervolgens de gebruikersreferenties met EAP-FAST en biedt toegang tot de draadloze clients.

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. Klik vervolgens op **Nieuw** om een RADIUS-server te definiëren.
2. Definieer de RADIUS-serverparameters op de **RADIUS-verificatieservers > Nieuwe** pagina. Deze parameters omvatten: IP-adres voor RADIUS-server Gedeeld geheim Poortnummer Serverstatus Dit document gebruikt de ACS-server met een IP-adres van 10.7.244.196.

The screenshot shows the Cisco WLC GUI configuration page for a new RADIUS Authentication Server. The page is titled "RADIUS Authentication Servers > New" and includes the following fields and options:

- Server Index (Priority): 1
- Server IP Address: 10.77.244.196
- Shared Secret Format: ASCII
- Shared Secret: \*\*\*\*\*
- Confirm Shared Secret: \*\*\*\*\*
- Key Wrap:  (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:  Enable
- Management:  Enable
- IPsec:  Enable

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

## [Configureer de WLAN voor WPA2 Enterprise Mode](#)

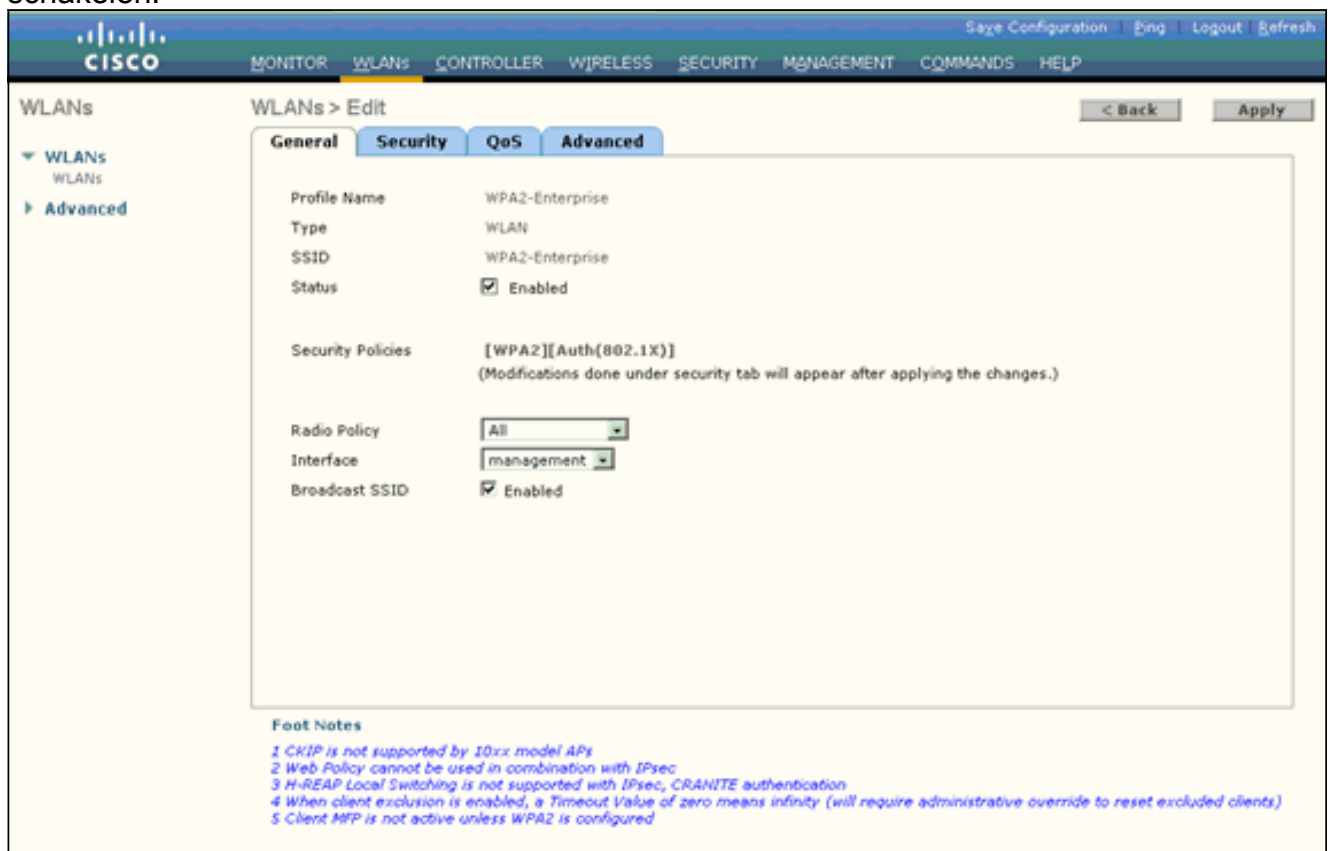
Configureer vervolgens het WLAN dat de clients zullen gebruiken om verbinding met het draadloze netwerk te maken. De WLAN SSID voor WPA2-Enterprise zal WPA2-Enterprise zijn. Dit voorbeeld wijst dit WLAN toe aan de beheerinterface.

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

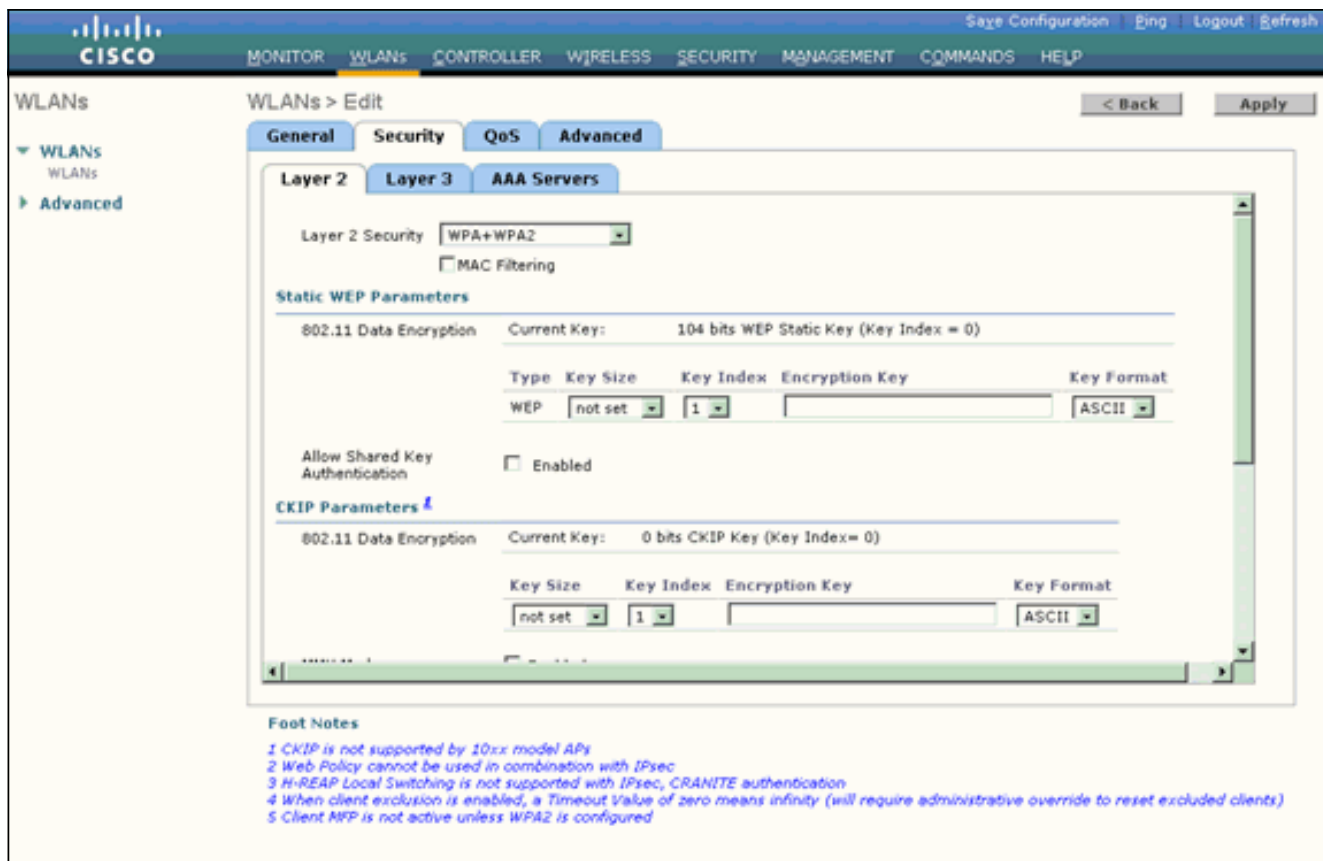
1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN-pagina weer te geven. Deze pagina maakt een lijst van de WLAN's die op de controller bestaan.
2. Klik op **Nieuw** om een nieuw WLAN te maken.
3. Voer de WLAN SSID-naam en de profielnaam in op de **WLAN's > Nieuwe** pagina. Klik vervolgens op **Toepassen**. Dit voorbeeld gebruikt **WPA2-Enterprise** als de SSID.



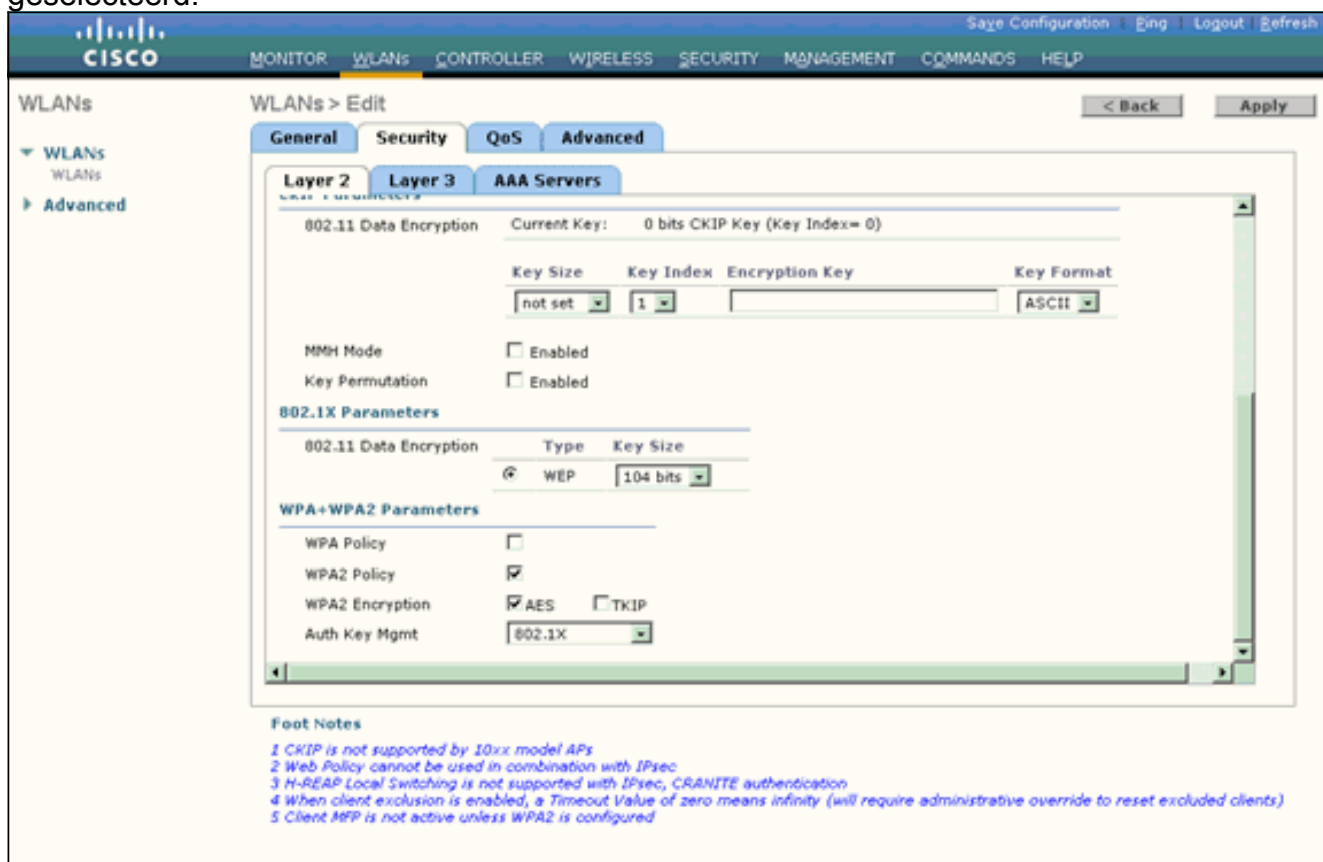
4. Zodra u een nieuw WLAN maakt, wordt de pagina **WLAN > Bewerken** voor het nieuwe WLAN weergegeven. Op deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN. Dit omvat Algemeen Beleid, Beveiligingsbeleid, QoS-beleid en Geavanceerde parameters.
5. Onder Algemeen beleid schakelt u het selectievakje **Status** in om het WLAN in te schakelen.



6. Als u wilt dat het toegangspunt de SSID uitzendt in de beacon-frames, vinkt u het aanvinkvakje **Broadcast SSID** aan.
7. Klik op het tabblad **Beveiliging**. Kies onder Layer 2 Security de optie **WPA+WPA2**. Dit schakelt WPA-verificatie in voor het WLAN.



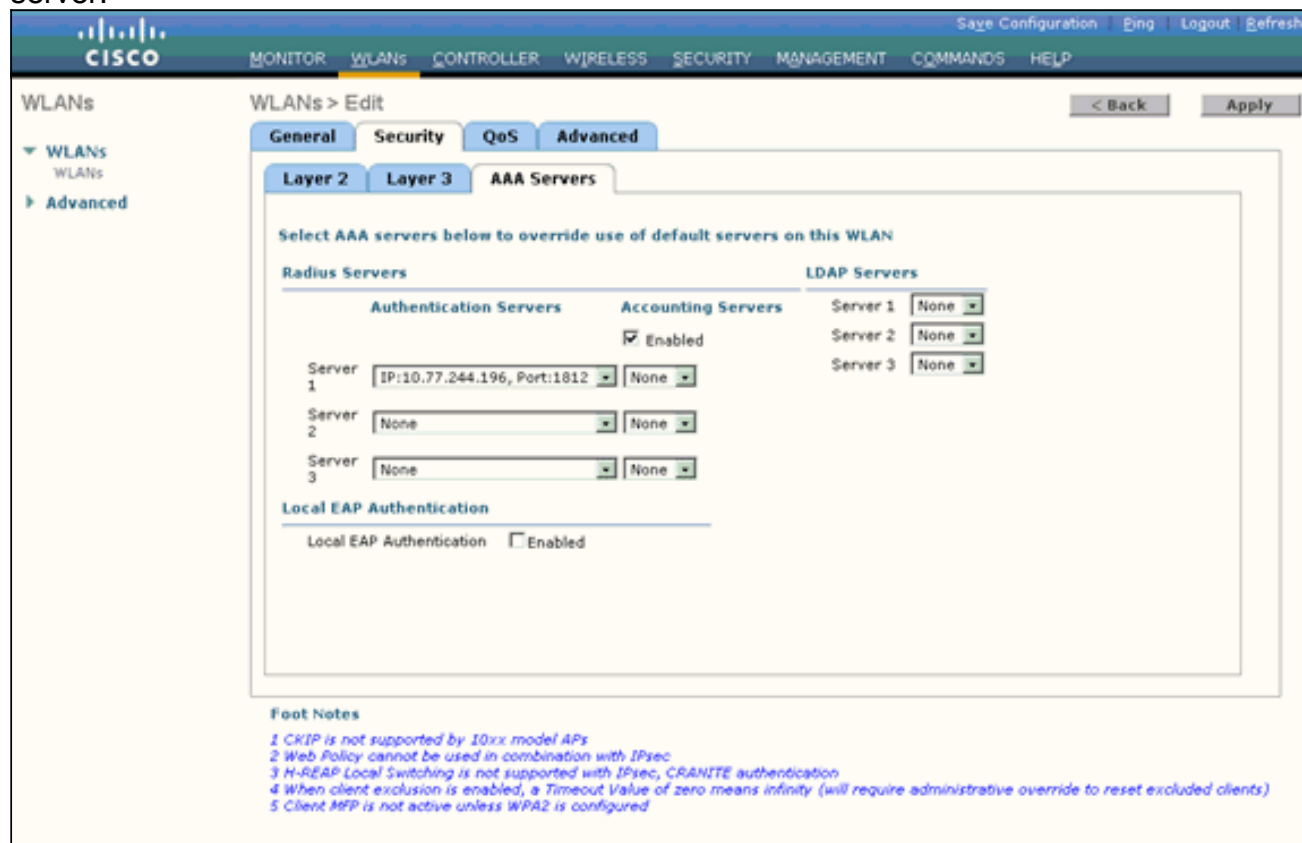
8. Blader naar beneden om de **WPA+WPA2-parameters** aan te passen. In dit voorbeeld zijn WPA2 Policy en AES encryptie geselecteerd.



9. Kies onder Auth Key Management **802.1x**. Dit schakelt WPA2 in met 802.1x/EAP-verificatie en AES-encryptie voor het WLAN.
10. Klik op het tabblad **AAA-servers**. Kies onder Verificatieservers het juiste IP-adres van de server. In dit voorbeeld wordt 10.77.24.196 gebruikt als de RADIUS-



server.



11. Klik op **Apply** (Toepassen). **Opmerking:** dit is de enige EAP-instelling die op de controller moet worden geconfigureerd voor EAP-verificatie. Alle andere configuraties die specifiek zijn voor EAP-FAST, moeten worden uitgevoerd op de RADIUS-server en de clients die moeten worden geverifieerd.

## [De RADIUS-server voor WPA2 Enterprise Mode-verificatie configureren \(EAP-FAST\)](#)

In dit voorbeeld wordt Cisco Secure ACS gebruikt als de externe RADIUS-server. Voer de volgende stappen uit om de RADIUS-server te configureren voor EAP-FAST-verificatie:

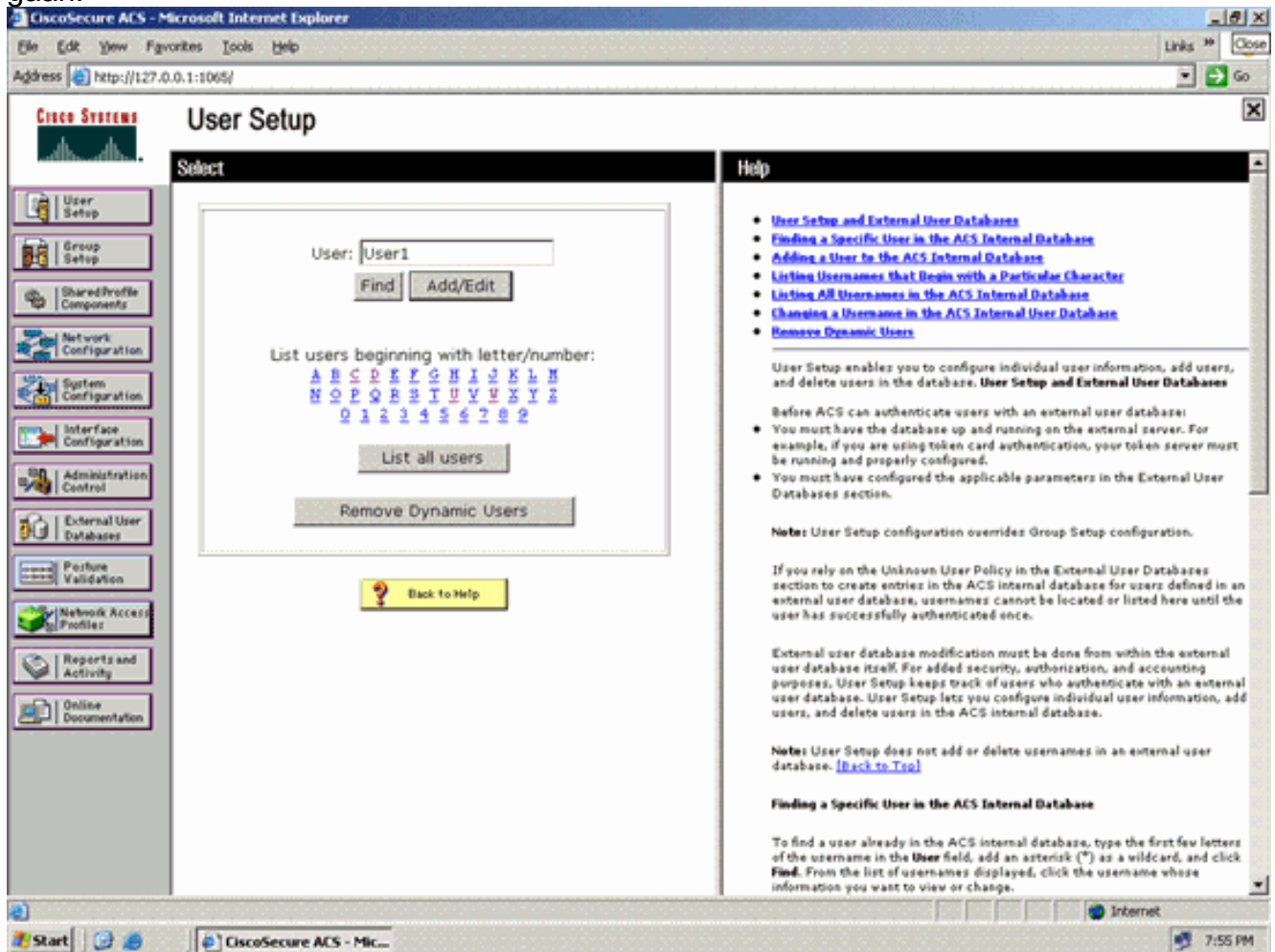
1. [Een gebruikersdatabase maken om clients te verifiëren](#)
2. [Voeg de WLC als AAA-client toe aan de RADIUS-server](#)
3. [EAP-FAST-verificatie op de RADIUS-server configureren met anonieme in-band PAC-provisioning](#) **Opmerking:** EAP-FAST kan worden geconfigureerd met Anonymous In-band PAC Provisioning of Authenticated In-band PAC Provisioning. In dit voorbeeld wordt anonieme in-band PAC Provisioning gebruikt. Zie [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](#).

### [Een gebruikersdatabase maken voor verificatie van EAP-FAST-clients](#)

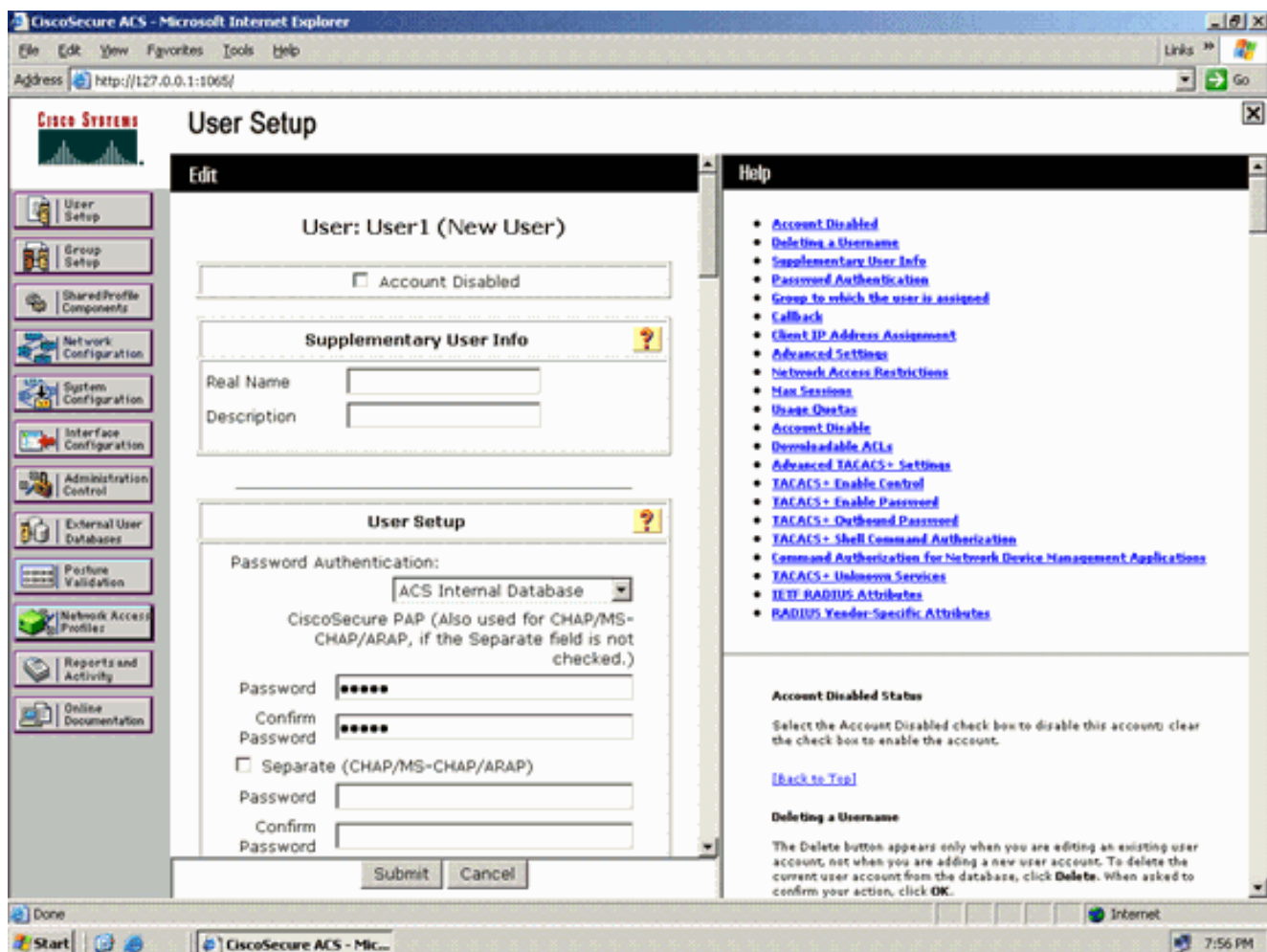
Voltooi deze stappen om een gebruikersdatabase te maken voor EAP-FAST-clients op de ACS. In dit voorbeeld worden de gebruikersnaam en het wachtwoord van de EAP-FAST-client respectievelijk ingesteld als Gebruiker1 en Gebruiker1.



1. Selecteer vanuit de ACS GUI in de navigatiebalk de optie **Gebruikersinstelling**. Maak een nieuwe draadloze gebruiker en klik vervolgens op **Toevoegen/Bewerken** om naar de pagina Bewerken van deze gebruiker te gaan.



2. Van de Instelling van de Gebruiker Bewerk pagina, vorm Echte Naam en Beschrijving evenals de Wachtwoordinstellingen zoals in dit voorbeeld. Dit document maakt gebruik van **ACS Interne Database** voor wachtwoordverificatie.

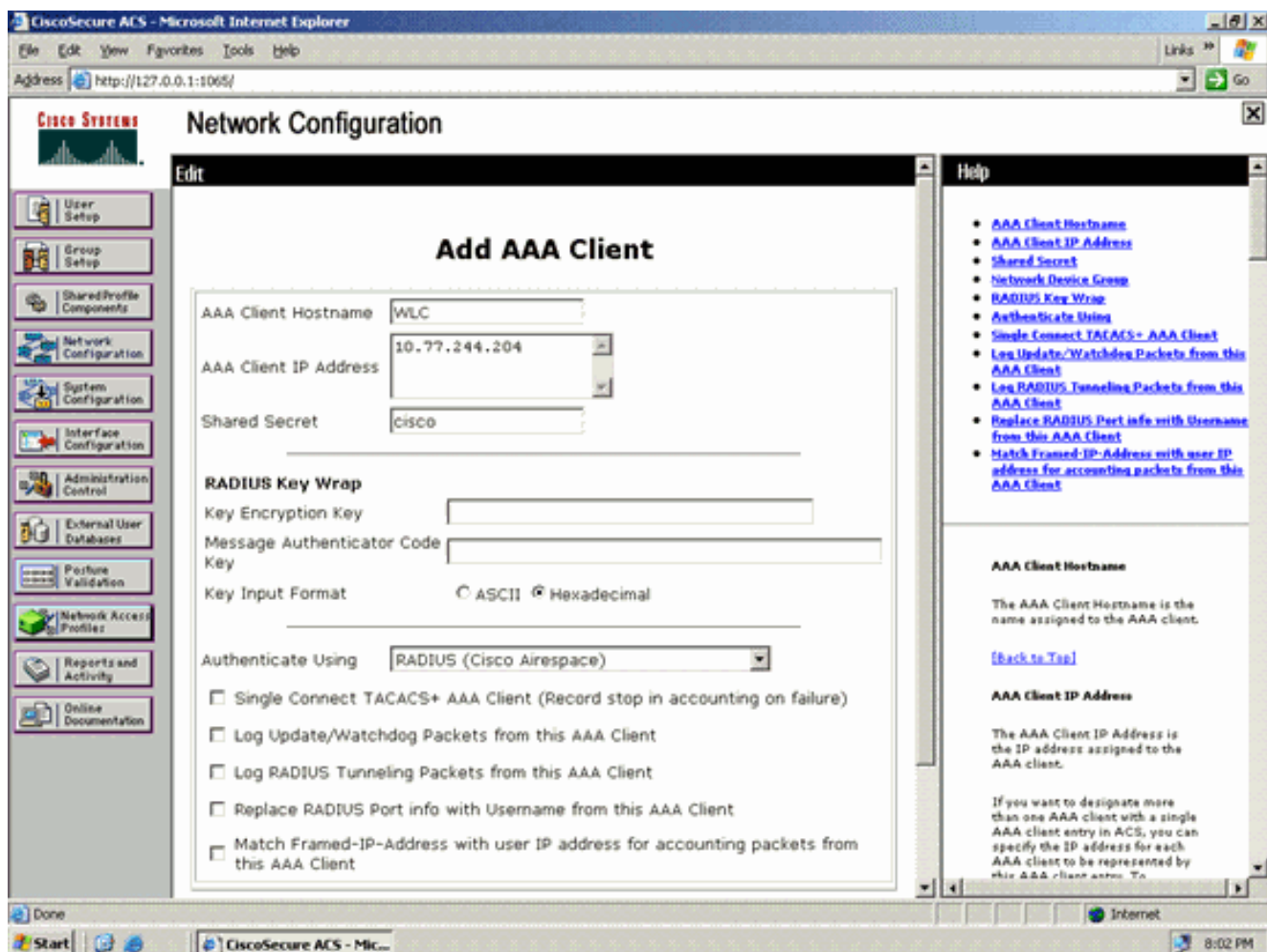


3. Kies **ACS Interne Database** uit de vervolgkeuzelijst Wachtwoordverificatie.
4. Configureer alle andere vereiste parameters en klik op **Indienen**.

### [Voeg de WLC als AAA-client toe aan de RADIUS-server](#)

Voltooi deze stappen om de controller te definiëren als een AAA-client op de ACS-server:

1. Klik op **Netwerkconfiguratie** vanuit de ACS GUI. Klik onder de sectie AAA-client toevoegen op de pagina Netwerkconfiguratie op **Add Entry** om WLC als AAA-client aan de RADIUS-server toe te voegen.
2. Definieer op de AAA-clientpagina de naam van de WLC, het IP-adres, de gedeelde geheimen verificatiemethode (RADIUS/Cisco Aironet). Raadpleeg de documentatie van de fabrikant voor andere niet-ACS-verificatieservers.



**Opmerking:** De gedeelde geheime sleutel die u op de WLC en de ACS-server configureren moet overeenkomen. Het gedeelde geheim is hoofdlettergevoelig.

3. Klik op **Indienen+Toepassen**.

## [EAP-FAST-verificatie op de RADIUS-server configureren met anonieme in-band PAC-provisioning](#)

### Anonieme in-band provisioning

Dit is een van de twee in-band provisioningmethoden waarin de ACS een beveiligde verbinding met de eindgebruiker-client tot stand brengt met als doel de klant een nieuwe PAC te geven. Deze optie maakt een anonieme TLS-handdruk mogelijk tussen de eindgebruiker client en ACS.

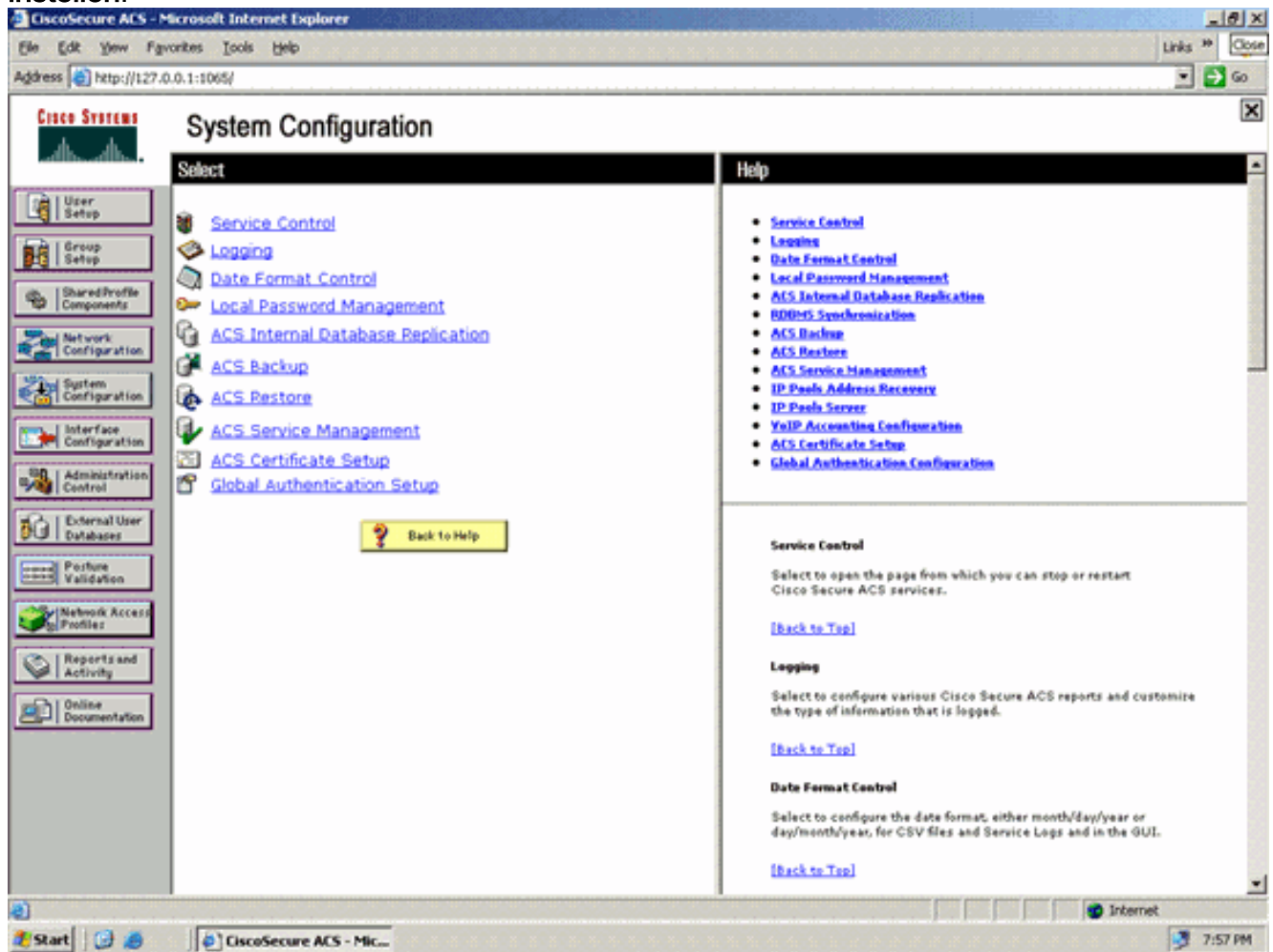
Deze methode werkt in een geverifieerde Diffie-Hellman-Key Overeenkomst Protocol (ADHP)-tunnel voordat de peer de ACS-server authenticceert.

Voor de ACS is EAP-MS-CHAPv2-verificatie van de gebruiker vereist. Bij een succesvolle gebruikersverificatie creëert de ACS een Diffie-Hellman-tunnel met de eindgebruiker-client. De ACS genereert een PAC voor de gebruiker en verstuurt deze naar de eindgebruiker client in deze tunnel, samen met informatie over deze ACS. Bij deze provisioningmethode wordt EAP-MSCHAPv2 gebruikt als de verificatiemethode in fase nul en EAP-GTC in fase twee.

Omdat een niet-geverifieerde server is voorzien, is het niet mogelijk om een wachtwoord in onbewerkte tekst te gebruiken. Daarom kunnen alleen MS-CHAP referenties worden gebruikt binnen de tunnel. MS-CHAPv2 wordt gebruikt om de identiteit van de peer aan te tonen en om een PAC te ontvangen voor verdere verificatiesessies (EAP-MS-CHAP wordt alleen als interne methode gebruikt).

Voltooi deze stappen om EAP-FAST-verificatie in de RADIUS-server te configureren voor anonieme in-band provisioning:

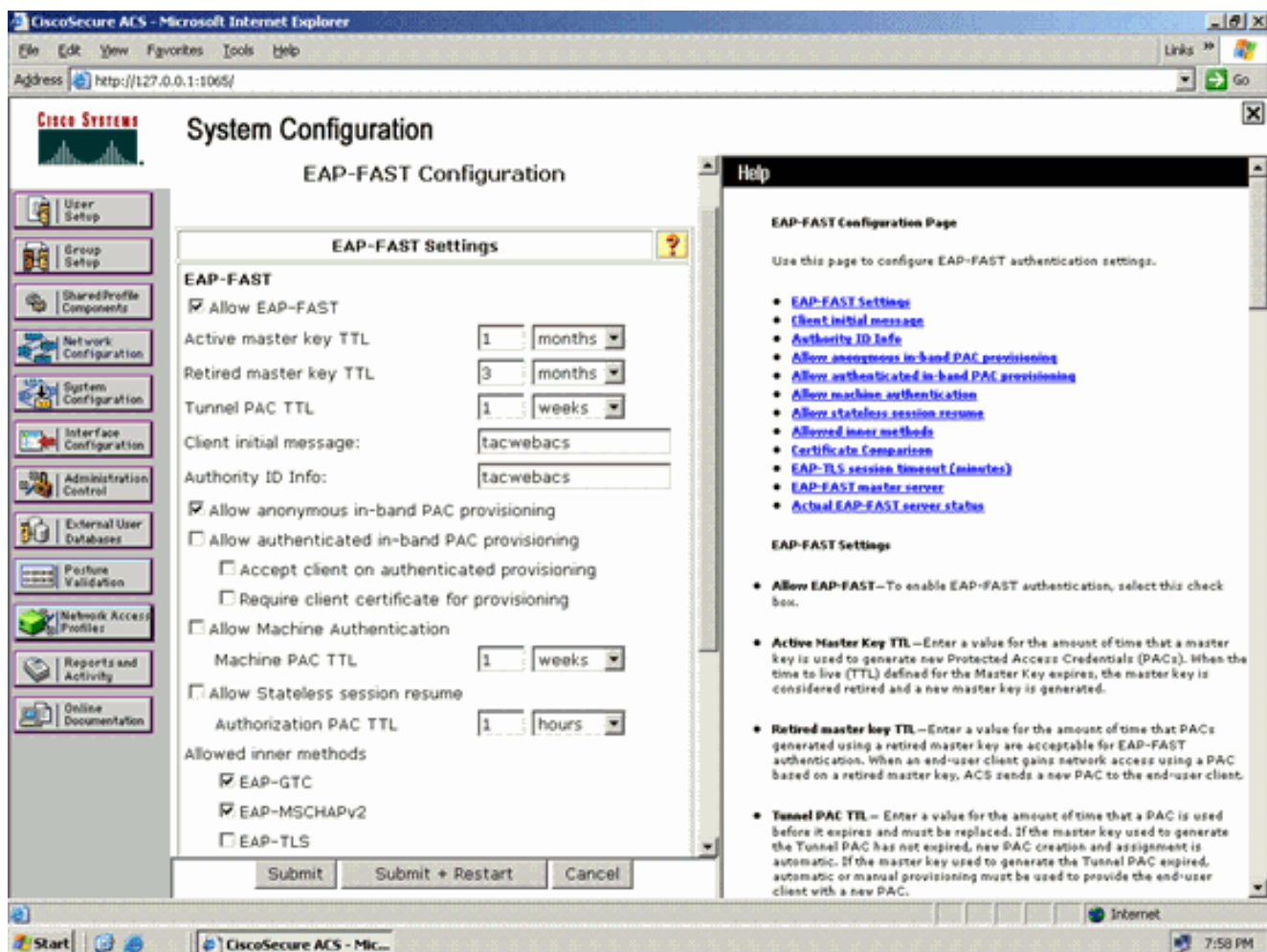
1. Klik op **Systeemconfiguratie** vanuit de RADIUS-server GUI. Kies op de pagina Systeemconfiguratie de optie **Globale verificatie instellen**.



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 te schakelen op de RADIUS-server.





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. Raadpleeg Master Keys voor meer informatie over actieve en uitgestelde master keys. Raadpleeg ook Master Keys en PAC TTL's voor meer informatie. 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. **Toegestane interne methoden**—Deze optie bepaalt welke interne EAP-methoden kunnen worden uitgevoerd binnen de EAP-FAST TLS-tunnel. 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.

## [De draadloze client voor WPA2 Enterprise Mode configureren](#)

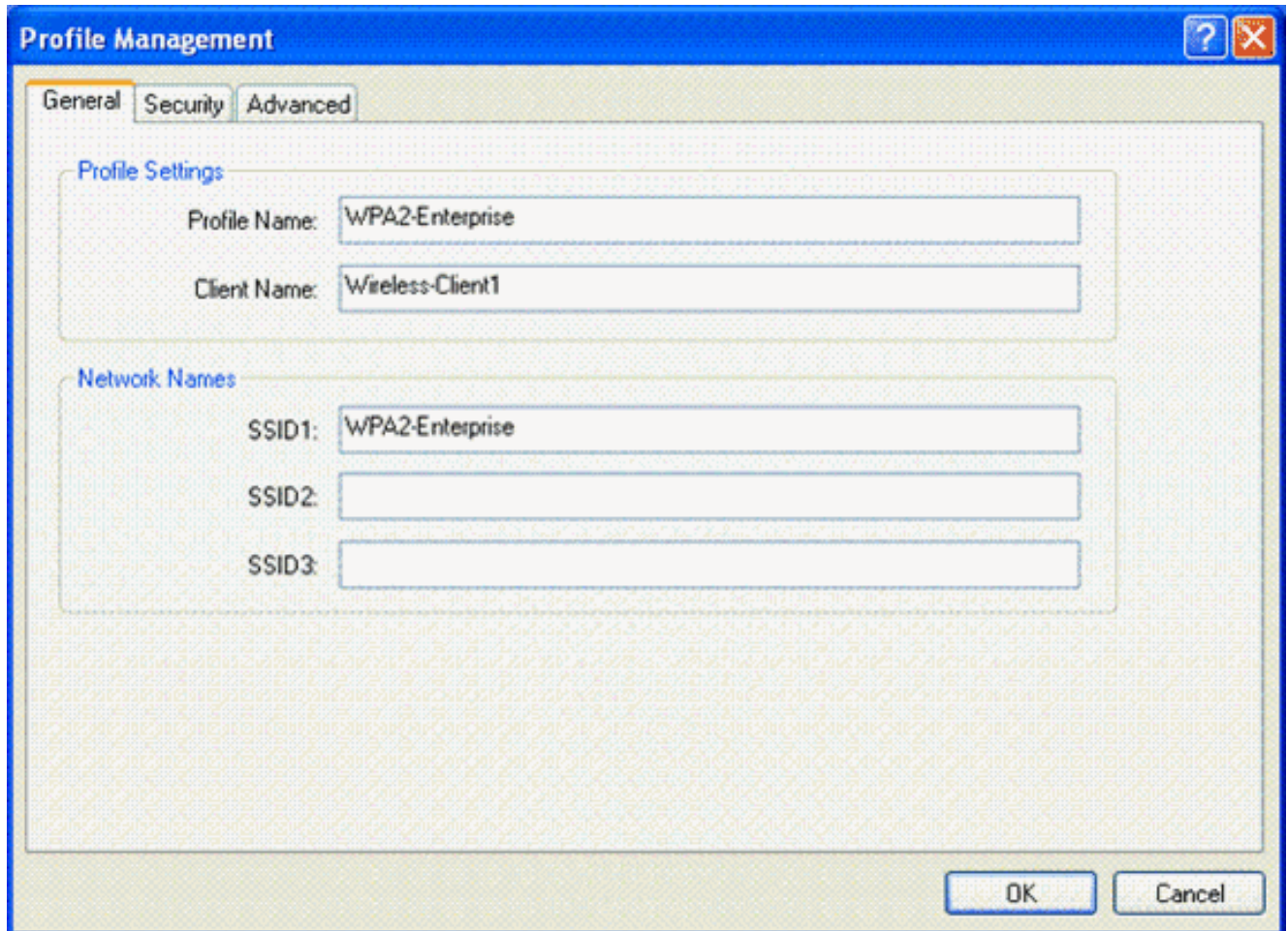
De volgende stap is het configureren van de draadloze client voor de modus WPA2 Enterprise.

Voltooi deze stappen om de draadloze client te configureren voor de WPA2 Enterprise-modus.

1. Klik vanuit het venster van het Aironet Desktop Utility op **Profielbeheer > Nieuw** om een profiel te maken voor de WPA2-Enterprise WLAN-gebruiker. Zoals eerder vermeld, gebruikt

dit document de WLAN/SSID-naam als **WPA2-Enterprise** voor de draadloze client.

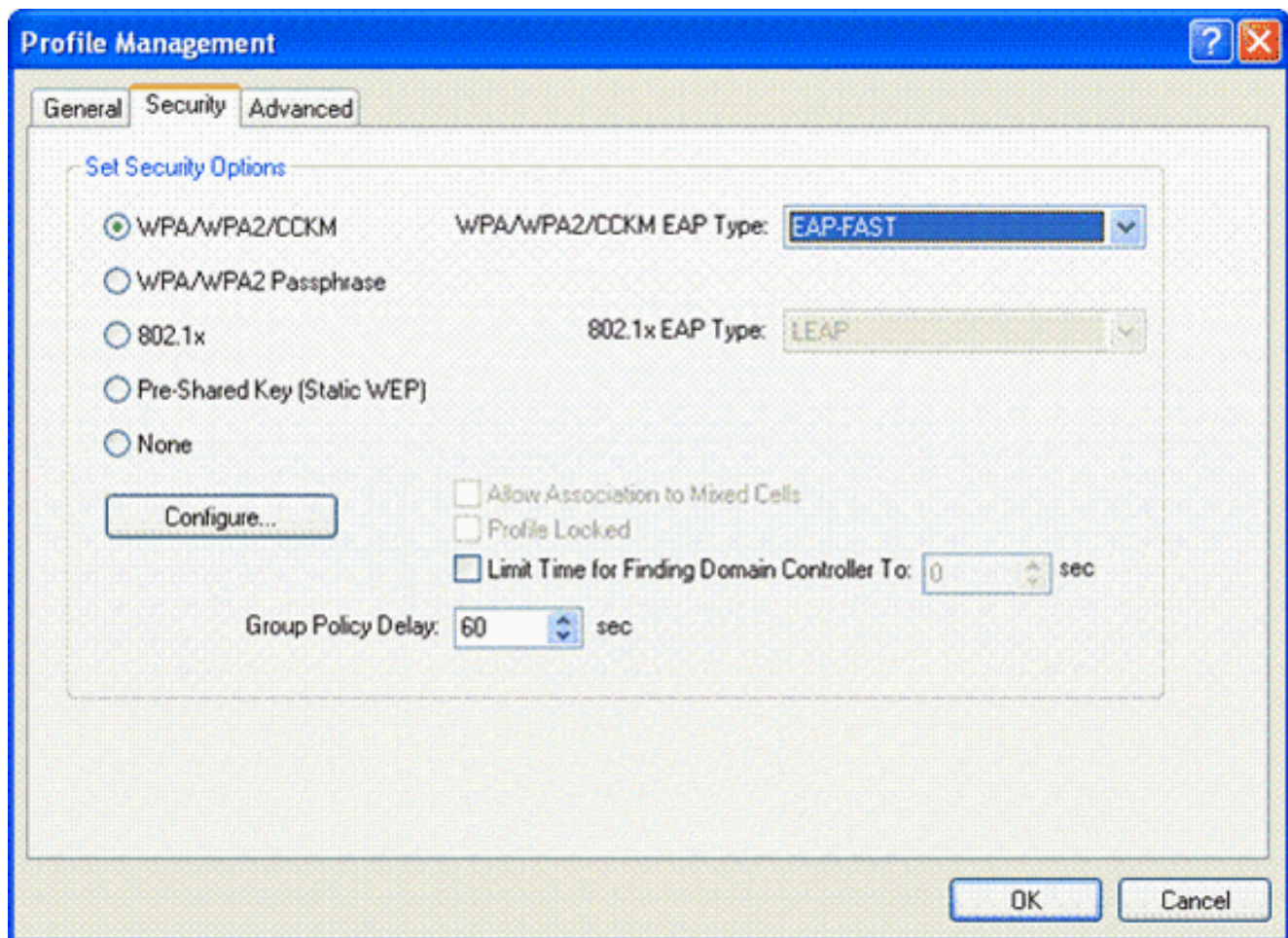
2. Klik vanuit het venster Profielbeheer op het tabblad **Algemeen** en configureer de profielnaam, de clientnaam en de SSID-naam zoals in dit voorbeeld. Klik vervolgens op **OK**



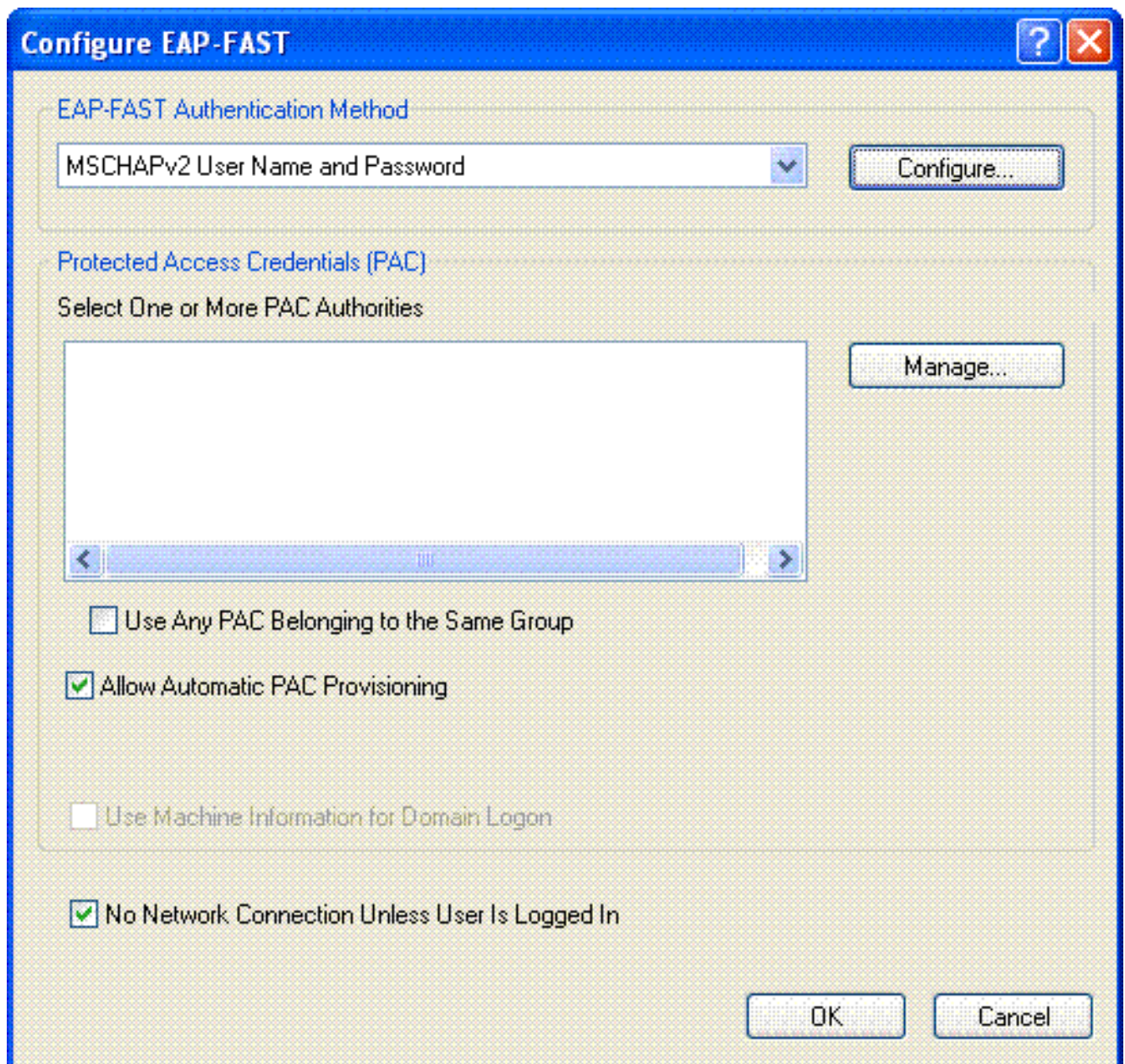
The screenshot shows a window titled "Profile Management" with three tabs: "General", "Security", and "Advanced". The "General" tab is selected. Under "Profile Settings", there are two text input fields: "Profile Name" containing "WPA2-Enterprise" and "Client Name" containing "Wireless-Client1". Under "Network Names", there are three text input fields: "SSID1" containing "WPA2-Enterprise", "SSID2" which is empty, and "SSID3" which is empty. At the bottom right, there are "OK" and "Cancel" buttons.

3. Klik op het tabblad **Beveiliging** en kies **WPA/WPA2/CCKM** om de WPA2-bedrijfsmodus in te schakelen. Kies onder WPA/WPA2/CCKM EAP-Type **EAP-FAST**. Klik op **Configureren** om de EAP-FAST-instelling te configureren.



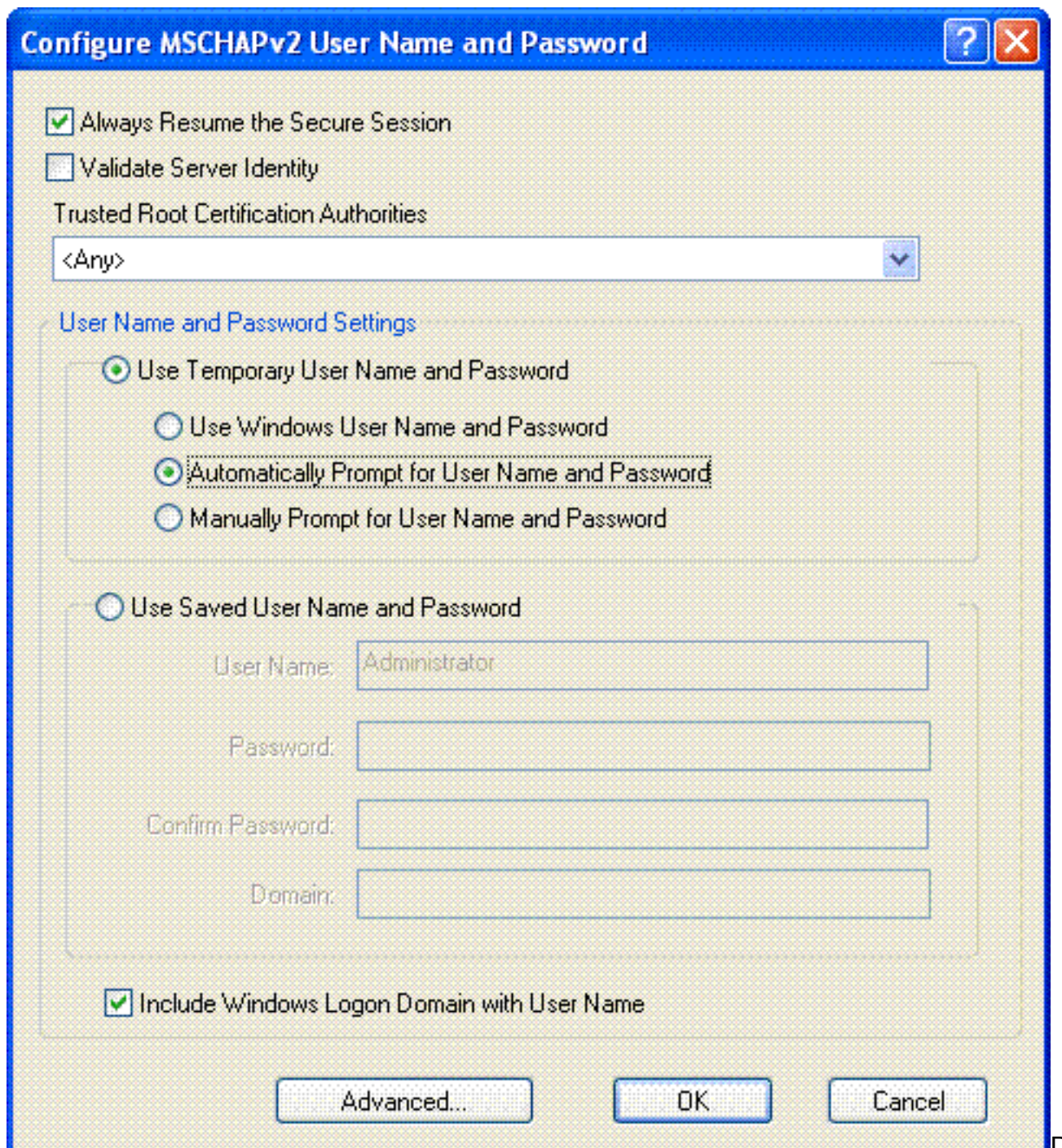


- Schakel in het venster EAP-FAST configureren het aanvinkvakje **Automatisch PAC-provisioning toestaan** in. Als u anonieme PAC-levering wilt configureren, wordt EAP-MS-CHAP gebruikt als de enige interne methode in fase nul.



5. Kies MSCHAPv2 Gebruikersnaam en wachtwoord als verificatiemethode in het vervolgkeuzevenster EAP-FAST-verificatiemethode. Klik op **Configureren**.
6. Kies in het venster Gebruikersnaam en wachtwoord instellen voor MSCHAPv2 de juiste gebruikersnaam en wachtwoord. In dit voorbeeld wordt **automatisch om gebruikersnaam en wachtwoord gevraagd**.





ezelfde gebruikersnaam en wachtwoord dienen te worden geregistreerd bij de ACS. Zoals eerder vermeld, gebruikt dit voorbeeld respectievelijk Gebruiker1 en Gebruiker1 als gebruikersnaam en wachtwoord. Merk ook op dat dit een anonieme in-band levering is. Daarom kan de client het servercertificaat niet valideren. U dient ervoor te zorgen dat het aanvinkvakje Server Identity valideren niet is ingeschakeld.

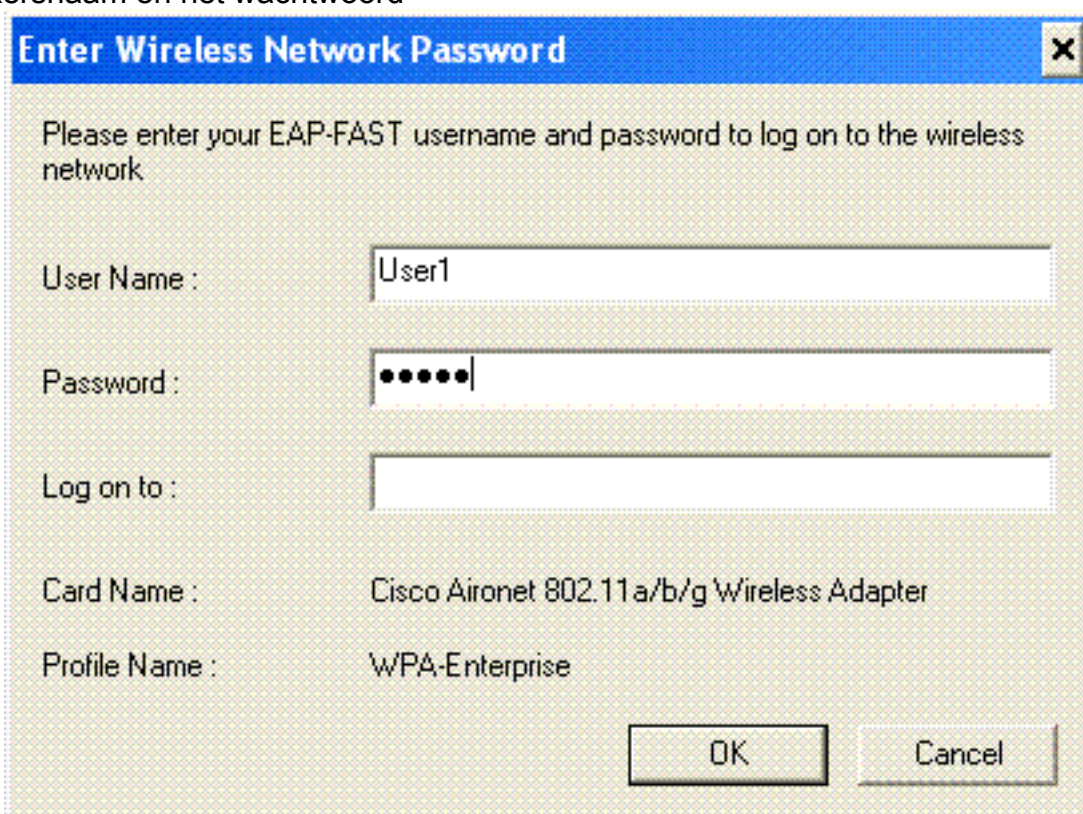
7. Klik op **OK**.

### [Controleer de activiteitsmodus van WPA2 Enterprise.](#)

Voltooi deze stappen om te verifiëren of uw configuratie van de WPA2 Enterprise-modus correct werkt:

1. Selecteer in het venster van het Aironet Desktop Utility het profiel **WPA2-Enterprise** en klik op **Activeren** om het profiel van de draadloze client te activeren.
2. Als u MS-CHAP ver2 hebt ingeschakeld als uw verificatie, zal de client u om de

gebruikersnaam en het wachtwoord



Enter Wireless Network Password

Please enter your EAP-FAST username and password to log on to the wireless network

User Name : User1

Password : ●●●●●●

Log on to :

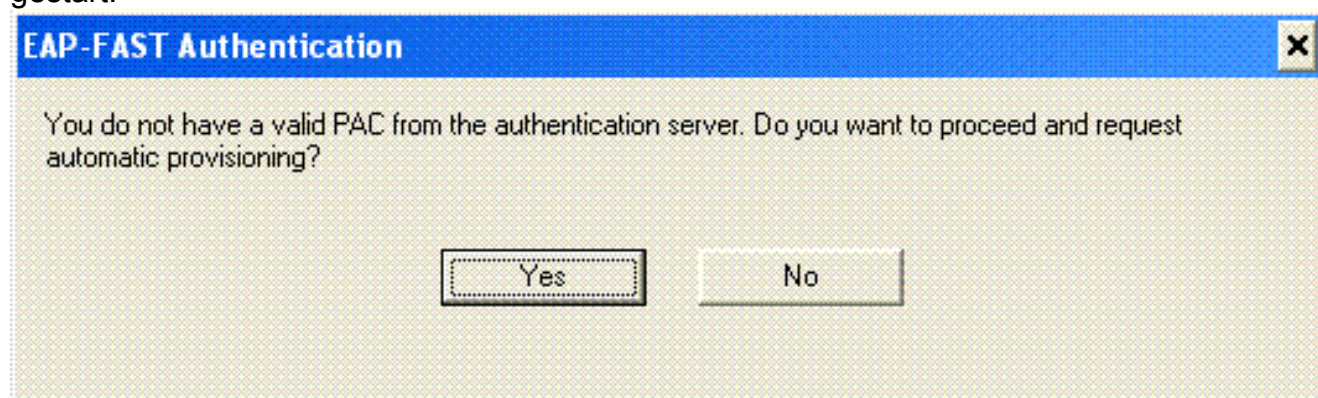
Card Name : Cisco Aironet 802.11 a/b/g Wireless Adapter

Profile Name : WPA-Enterprise

OK Cancel

vragen.

3. Tijdens EAP-FAST-verwerking van de gebruiker wordt u door de client gevraagd om PAC aan te vragen bij de RADIUS-server. Wanneer u op **Ja** klikt, wordt de PAC-provisioning gestart.

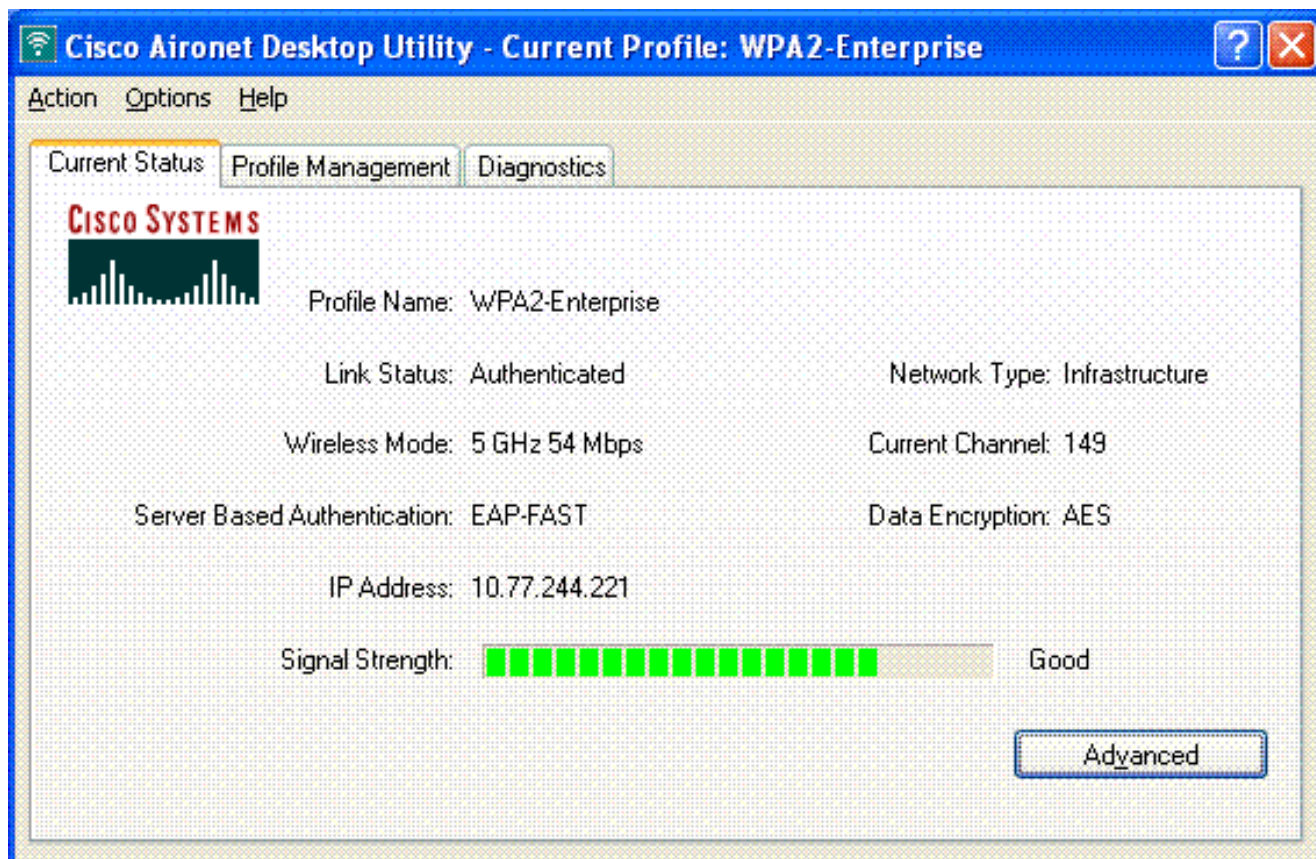


EAP-FAST Authentication

You do not have a valid PAC from the authentication server. Do you want to proceed and request automatic provisioning?

Yes No

4. Na succesvolle PAC-levering in fase nul volgen fase één en twee en vindt een succesvolle verificatieprocedure plaats. Na succesvolle verificatie wordt de draadloze client gekoppeld aan WLAN WPA2-Enterprise. Dit is de screenshot:



U kunt ook controleren of de RADIUS-server het verificatieverzoek van de draadloze client ontvangt en valideert. Controleer de Overgegaan Verificaties en de Ontbroken rapporten van Pogingen over de server ACS om dit te verwezenlijken. Deze rapporten zijn beschikbaar onder Rapporten en Activiteiten op de ACS-server.

## [De apparaten configureren voor WPA2 Personal Mode](#)

Voer deze stappen uit om de apparaten te configureren voor de WPA2-Personal-werkmodus:

1. [Het WLAN configureren voor WPA2 Personal Mode-verificatie](#)
2. [De draadloze client configureren voor WPA2 Personal Mode](#)

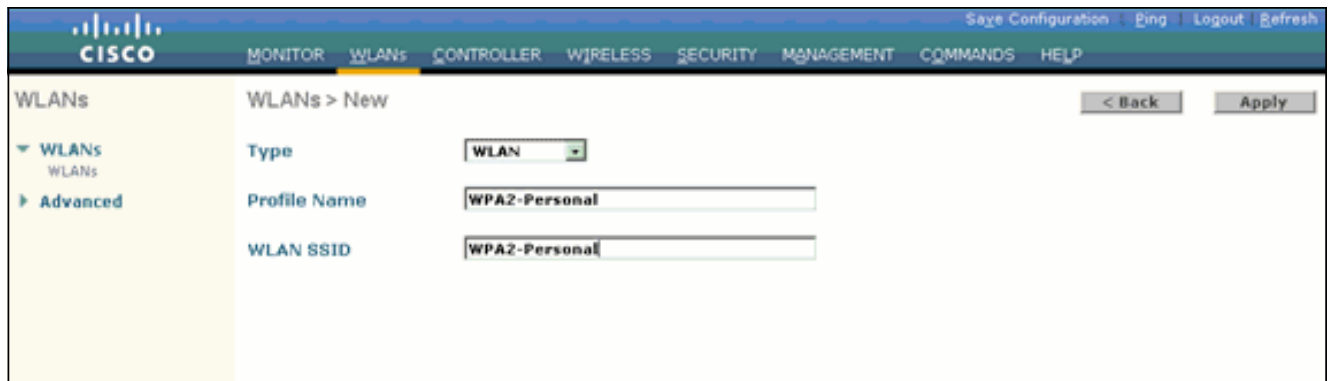
### [Configureer de WLAN voor WPA2 Personal Mode](#)

U moet het WLAN configureren dat de clients zullen gebruiken om verbinding te maken met het draadloze netwerk. De WLAN SSID voor WPA2 Personal-modus is WPA2-Personal. Dit voorbeeld wijst dit WLAN toe aan de beheerinterface.

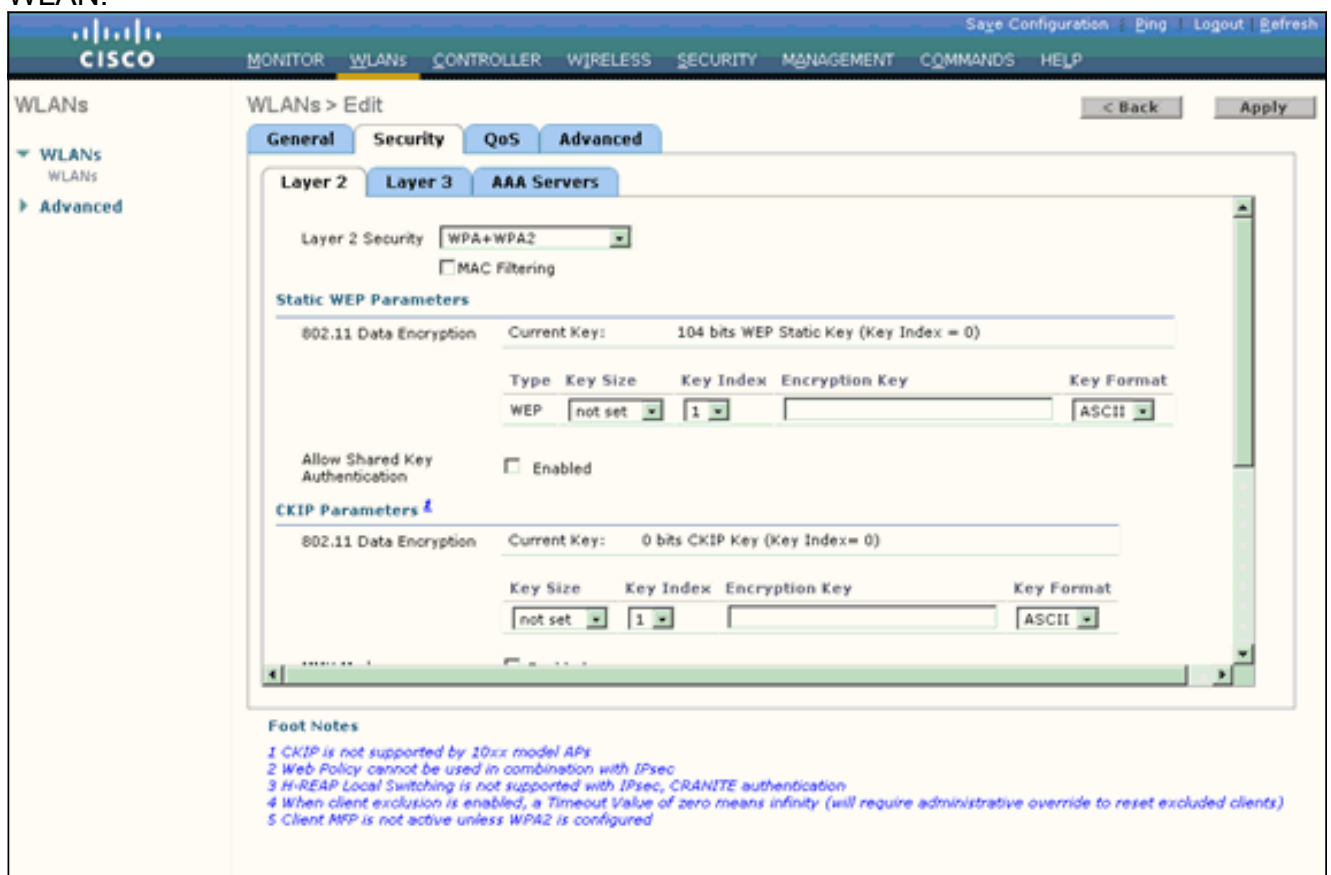
Voltooi deze stappen om WLAN en de bijbehorende parameters te configureren:

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.
3. Voer op de WLAN's > Nieuwe pagina de WLAN-SSID-naam, de profielnaam en de WLAN-id in. Klik vervolgens op **Toepassen**. Dit voorbeeld gebruikt **WPA2-Personal** als de SSID.





4. 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, Beveiligingsbeleid, QoS-beleid en Geavanceerde parameters.
5. Onder Algemeen beleid schakelt u het selectievakje **Status** in om het WLAN in te schakelen.
6. Als u wilt dat het toegangspunt de SSID uitzendt in de beacon-frames, vinkt u het aanvinkvakje **Broadcast SSID** aan.
7. Klik op het tabblad **Beveiliging**. Kies onder Layer Security de optie **WPA+WPA2**. Dit schakelt WPA-verificatie in voor het WLAN.



8. Blader naar beneden om de **WPA+WPA2-parameters** aan te passen. In dit voorbeeld zijn WPA2 Policy en AES encryptie geselecteerd.
9. Kies onder Auth Key Management **PSK** om WPA2-PSK in te schakelen.
10. Voer de vooraf gedeelde sleutel in het juiste veld in zoals aangegeven in de afbeelding.

WLANs > Edit

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Key Size: not set Key Index: 1 Encryption Key: Key Format: ASCII

MMH Mode:  Enabled  
Key Permutation:  Enabled

802.1X Parameters

802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	104 bits

WPA+WPA2 Parameters

WPA Policy:   
WPA2 Policy:   
WPA2 Encryption:  AES  TKIP  
Auth Key Mgmt: PSK  
PSK Format: ASCII

Foot Notes

1 TKIP is not supported by 10xx model APs  
2 Web Policy cannot be used in combination with IPsec  
3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication  
4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)  
5 Client MFP is not active unless WPA2 is configured

**Opmerking:** Vooraf gedeelde sleutel die gebruikt wordt op de WLC moet overeenkomen met de sleutel die geconfigureerd is op de draadloze clients.

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

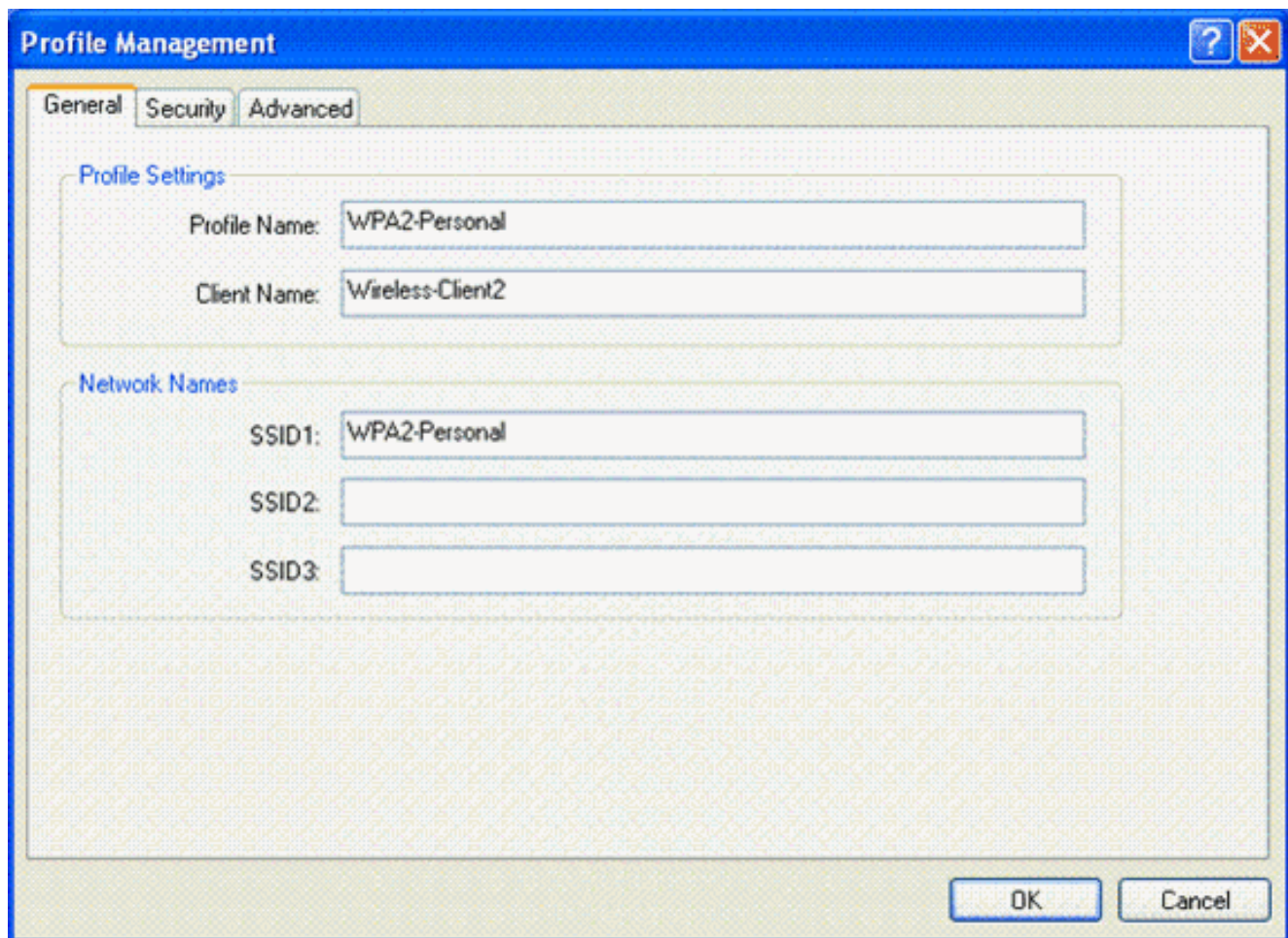
### [De draadloze client configureren voor WPA2 Personal Mode](#)

De volgende stap is het configureren van de draadloze client voor de WPA2-Personal-modus.

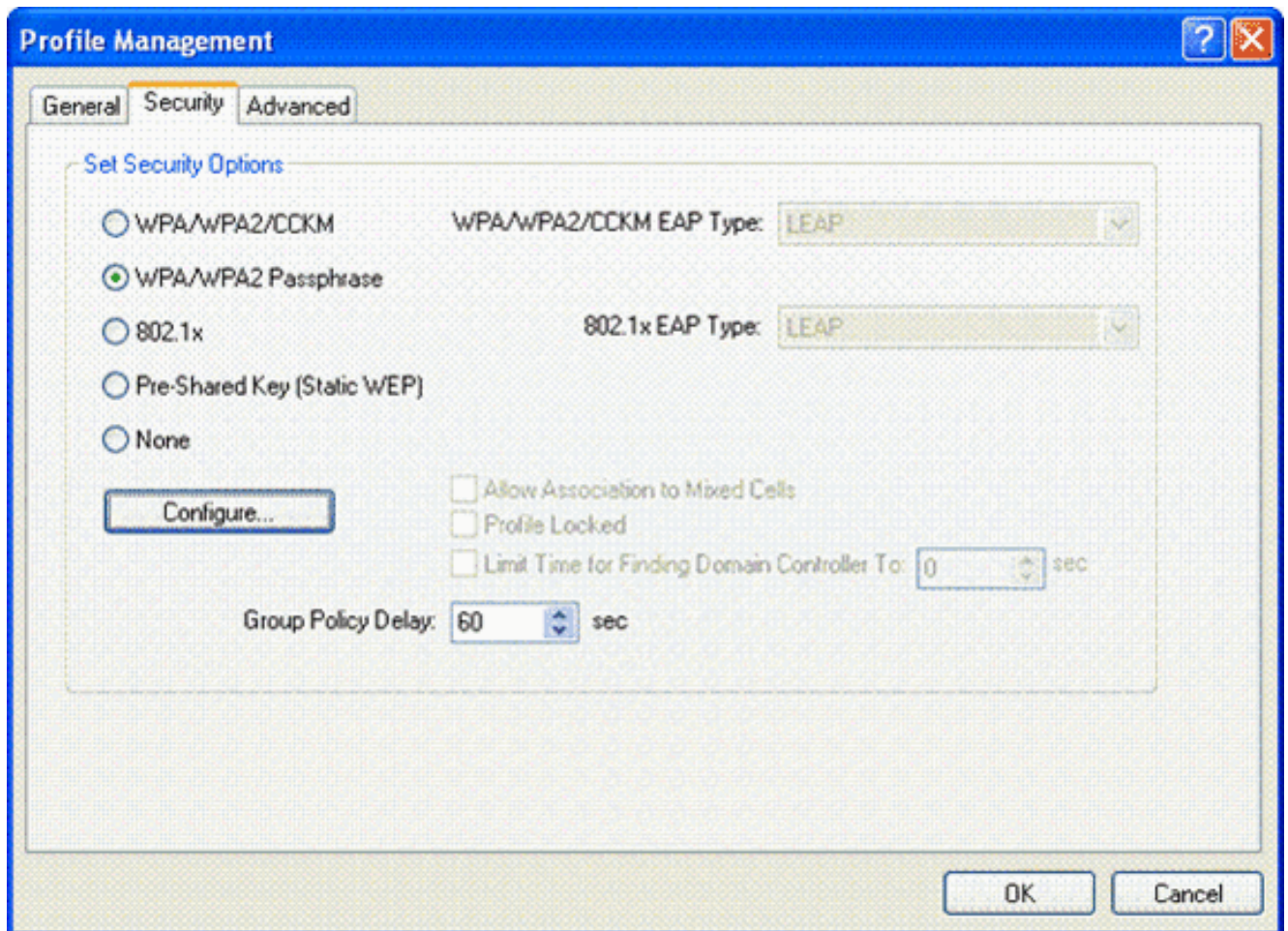
Voltooi deze stappen om de draadloze client te configureren voor de WPA2-Personal-modus:

1. Klik vanuit het venster van het Aironet Desktop Utility op **Profile Management > New** om een profiel te maken voor WPA2-PSK WLAN-gebruiker.
2. Klik vanuit het venster Profielbeheer op het tabblad **Algemeen** en configureer de profielnaam, de clientnaam en de SSID-naam zoals in dit voorbeeld. Klik vervolgens op **OK**.

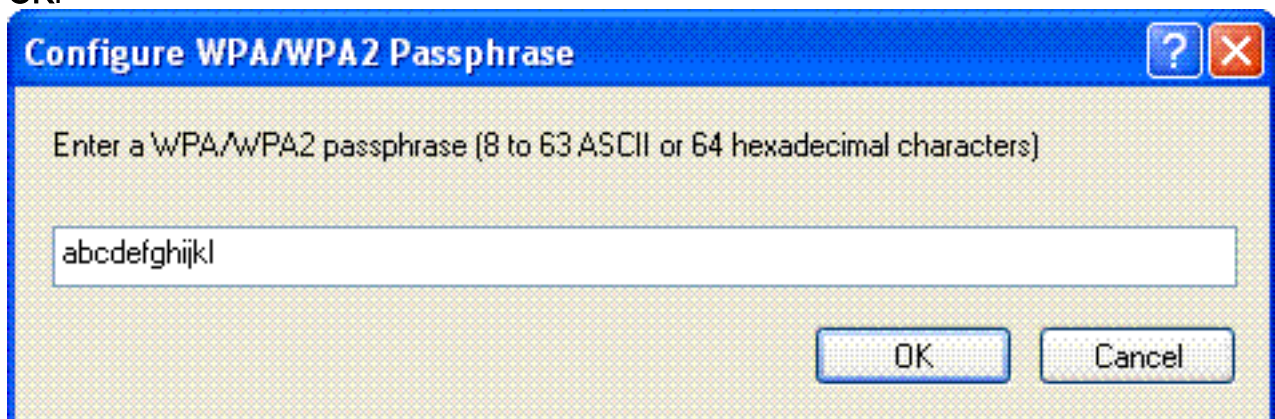




3. Klik op het tabblad **Beveiliging** en kies **WPA/WPA2-wachtwoordgroep** om de werkwijze van WPA2-PSK in te schakelen. Klik op **Configureren** om de voorgedeelde sleutel met WPA-PSK te configureren.



4. Voer de vooraf gedeelde toets in en klik op OK.



### [Verifieer de WPA2-Personal-modus van de handeling](#)

Voltooi deze stappen om te verifiëren of uw WPA2-Enterprise-modemconfiguratie correct werkt:

1. Selecteer in het venster van het Aironet Desktop Utility het profiel **WPA2-Personal** en klik op **Activeren** om het profiel van de draadloze client te activeren.
2. Nadat het profiel is geactiveerd, wordt de draadloze client bij de WLAN aangesloten op een succesvolle verificatie. Dit is de screenshot:





Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**

Wed Feb 20 14:20:00 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)**

Wed Feb 20 14:20:01 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)**

Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -0

Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3689 seconds on AP 00:0b:85:91:c3:c0

Wed Feb 20 14:20:29 2007: Creating dot1x interface with key 00:0b:85:91:c3:c0 -1

Wed Feb 20 14:20:29 2007: Resetting the group key timer for 3696 seconds on AP 00:0b:85:91:c3:c0

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 22)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received Identity Response (count=3) from mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ==> 19 for STA 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 19)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 19, EAP Type 3)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 43)

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:30 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 23)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 23, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 26)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 26, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 27)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 27, EAP Type 43)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Processing Access-Reject for mobile00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Failure to mobile 00:4096:af:3e:93 (EAP Id 27)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Setting quiet timer for 5 seconds for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 1)

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Received EAPOL START from mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:31 2007: 00:40:96:af:3e:93 Sending EAP-Request/Identity to mobile 00:40:96:af:3e:93 (EAP Id 2)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Identity Response (count=2) from mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 2 ==> 20 for STA 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 20)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 20, EAP Type 3)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 21)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 21, EAP Type 43)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 22)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 22, EAP Type 43)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Processing Access-Challenge for mobile 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 WARNING: updated EAP-Identifer 22 ==> 24 for STA 00:40:96:af:3e:93

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 24)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 24, EAP Type 43)

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Challenge for mobile 00:40:96:af:3e:93**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Sending EAP Request from AAA to mobile 00:40:96:af:3e:93 (EAP Id 25)**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Received EAP Response from mobile 00:40:96:af:3e:93 (EAP Id 25, EAP Type 43)**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Processing Access-Accept for mobile 00:40:96:af:3e:93**

Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 **Creating a new PMK Cache Entry for tation 00:40:96:af:3e:93 (RSN 0)**

```
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending EAP-Success to  
mobile 00:40:96:af:3e:93 (EAP Id 25)  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending default RC4 key to  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Sending Key-Mapping RC4 key to  
mobile 00:40:96:af:3e:93  
Wed Feb 20 14:20:32 2007: 00:40:96:af:3e:93 Received Auth Success while in  
Authenticating state for mobile 00:40:96:af:3e:93
```

- **debug dot1x-pakket-inschakelen**-Hiermee kunt u debug van 802.1x-pakketberichten inschakelen.
- **debug aaa gebeurtenissen enable**-Enabled de debug output van alle aaa gebeurtenissen.

## [Gerelateerde informatie](#)

- [WPA2 - Wi-Fi Protected Access 2](#)
- [EAP-FAST-verificatie met draadloze LAN-controllers en externe RADIUS-serverconfiguratievoorbeld](#)
- [Configuratie-voorbeeld van EAP-verificatie met WLAN-controllers \(WLC\)](#)
- [Overzicht van WPA-configuratie](#)
- [Ondersteuning voor wireless producten](#)
- [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.