

Configuratievoorbeeld van Wi-Fi Protected Access 2 (WAP 2)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[WAP 2-ondersteuning met Cisco Aironet-apparatuur](#)

[Configureren in ondernemingsmodus](#)

[Netwerkinstelling](#)

[AP configureren](#)

[CLI-configuratie](#)

[De clientadapter configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Instellen in persoonlijke modus](#)

[Netwerkinstelling](#)

[AP configureren](#)

[De clientadapter configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document verklaart de voordelen van het gebruik van Wi-Fi Protected Access 2 (WAP 2) in een draadloos LAN (WLAN). Het document biedt twee configuratievoorbeelden voor het implementeren van WAP 2 op een WLAN. Het eerste voorbeeld toont hoe te om WAP 2 in ondernemingsmodus te vormen, en het tweede voorbeeld vormt WAP 2 in persoonlijke modus.

Opmerking: WAP werkt met Extensible Authentication Protocol (EAP).

[Voorwaarden](#)

[Vereisten](#)

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

- medearbeidster
- WLAN-beveiligingsoplossingen **Opmerking:** Raadpleeg [Cisco Aironet draadloos 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 Aironet 1310G access point (AP)/brug die Cisco IOS® software release 12.3(2)JA runt
- Aironet 802.11a/b/g CB21AG clientadapter voor firmware 2.5
- Aironet Desktop Utility (ADU) dat firmware 2.5 uitvoert

Opmerking: De software van de Aironet CB21AG en PI21AG clientadaptersoftware is niet compatibel met de software van andere Aironet-clientadaptersoftware. U moet de ADU gebruiken met CB21AG- en PI21AG-kaarten en u moet de Aironet Client Utility (ACU) alle andere Aironet-clientadapters gebruiken. Raadpleeg [De clientadapter installeren](#) voor meer informatie over het installeren van de CB21AG-kaart en de ADU.

N.B.: Dit document gebruikt een AP/brug die een geïntegreerde antenne heeft. Als u een AP/brug gebruikt die een externe antenne vereist, zorg er dan voor dat de antennes op AP/brug worden aangesloten. Anders kan AP/bridge niet aan het draadloze netwerk verbinden. Bepaalde AP/bridge-modellen worden met geïntegreerde antennes geleverd, terwijl andere een externe antenne nodig hebben voor het algemeen gebruik. Raadpleeg voor informatie over de AP/bridge-modellen die met interne of externe antennes worden geleverd de bestelgeleider/producthandleiding van de juiste voorziening.

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

WAP is een op standaarden gebaseerde beveiligingsoplossing van de Wi-Fi Alliance die de kwetsbaarheden in inheemse WLAN's aanpakt. WAP biedt verbeterde gegevensbescherming en toegangscontrole voor WLAN-systemen. WAP richt zich op alle gekende kwetsbaarheden van de Geboden Equivalent Privacy (WLAN) in de originele de veiligheidsimplementatie van IEEE 802.11 en brengt een onmiddellijke veiligheidsoplossing aan WLANs in zowel onderneming als kleine (SOHO) omgevingen van het huiskantoor.

WAP 2 is de volgende generatie Wi-Fi-beveiliging. WAP 2 is de interoperabele implementatie van de geratificeerde standaard IEEE 802.11i. WAP 2 implementeert het door NIST (National Institute of Standards and Technology) aanbevolen Advanced Encryption Standard (AES)-encryptie-algoritme met het gebruik van Counter Mode met Cipher Block Chaining Message Authentication Protocol (CCMP). AES Counter Mode is een blok algoritme die gegevens met 128 bits tegelijk versleutelt met een 128-bits coderingssleutel. Het CCMP-algoritme produceert een

berichtintegriteitscode (MIC) die verificatie van gegevensoorsprong en gegevensintegriteit voor het draadloze frame biedt.

Opmerking: CCMP wordt ook CBC-MAC genoemd.

WAP 2 biedt een hoger beveiligingsniveau dan WAP omdat AES een sterkere codering biedt dan TKIP (Temporal Key Integrity Protocol). TKIP is het coderingsalgoritme dat WAP gebruikt. WAP 2 maakt verse sessiesleutels op elke associatie. De encryptiesleutels die voor elke client op het netwerk worden gebruikt, zijn uniek en specifiek voor die client. Uiteindelijk wordt elk pakje dat via de lucht wordt verstuurd, versleuteld met een unieke sleutel. De beveiliging wordt verbeterd door het gebruik van een nieuwe en unieke coderingssleutel omdat er geen sleutelhergebruik is. WAP wordt nog steeds als veilig beschouwd en TKIP is niet verbroken. Cisco raadt echter aan dat klanten zo snel mogelijk overschakelen naar WAP 2.

WAP en WAP 2 ondersteunen beide operationele modi:

- Enterprise-modus
- Persoonlijke modus

In dit document wordt de implementatie van deze twee modi besproken met WAP 2.

[WAP 2-ondersteuning met Cisco Aironet-apparatuur](#)

WAP 2 wordt ondersteund op deze apparatuur:

- Aironet 1130AG AP-serie en 1230AG AP-serie
- Aironet 1100 AP Series
- Aironet 1200 AP Series
- Aironet 1300 AP Series

Opmerking: Equip deze AP's met 802.11g radio's en gebruik Cisco IOS-software release 12.3(2)JA of hoger.

WAP 2 en AES worden ook ondersteund op:

- Aironet 1200 Series radiomodules met de onderdeelnummers AIR-RM21A en AIR-RM22A **Opmerking:** de Aironet 1200 radiomodules met het onderdeelnummer AIR-RM20A ondersteunen geen WAP 2.
- Aironet 802.11a/b/g clientadapters met firmware versie 2.5

Opmerking: Cisco Aironet 350 Series producten ondersteunen WAP 2 niet omdat hun radio's geen AES-ondersteuning hebben.

Opmerking: Cisco Aironet 1400 Series draadloze bruggen ondersteunen WAP 2 of AES niet.

[Configureren in ondernemingsmodus](#)

De term **ondernemingsmodus** verwijst naar producten die getest worden om interoperabel te zijn in zowel de pre-Shared Key (PSK) als de IEEE 802.1x-werkwijzen voor verificatie. 802.1x wordt als veiliger beschouwd dan elk van de erfenisauthenticatiekaders vanwege de flexibiliteit ter ondersteuning van een verscheidenheid aan authenticatiemechanismen en sterkere encryptie-algoritmen. WAP 2 voert in bedrijfsmodus verificatie uit in twee fasen. De configuratie van open authenticatie vindt plaats in de eerste fase. De tweede fase is 802.1x-authenticatie met één van

de MAP-methoden. AES biedt het coderingsmechanisme.

In de bedrijfsmodus zijn klanten en authenticatieservers elkaar authentiek met behulp van een MAP-verificatiemethode en genereren de cliënt en server een Pairwise Master Key (PMK). Met WAP 2 genereert de server dynamisch de PMK en geeft de PMK door aan de AP.

In dit gedeelte wordt de configuratie besproken die nodig is om WAP 2 in de bedrijfsmodus uit te voeren.

[Netwerkinstelling](#)

In deze opstelling, verklaart een Aironet 1310G AP/Bridge die Cisco Lichtgewicht Extensible Authentication Protocol (LEAP) runt een gebruiker met een WAP 2-compatibele clientadapter. Key Management vindt plaats met behulp van WAP 2, waarop AES-CCMP-encryptie is geconfigureerd. AP wordt gevormd als een lokale server van RADIUS die LEAP authenticatie uitvoert. U moet de clientadapter en de AP configureren om deze instelling uit te voeren. De secties [Configureer de AP](#) en [configureren de clientadapter](#) tonen de configuratie op het AP en de clientadapter.

[AP configureren](#)

Volg deze stappen om AP te configureren met behulp van GUI:

1. Configureer de AP als een lokale RADIUS-server met LEAP-verificatie. Kies **Security > Server Manager** in het menu links en definieer het IP-adres, poorten en gedeeld geheim van de RADIUS-server. Omdat deze configuratie AP als lokale RADIUS server vormt, gebruik het IP adres van AP. Gebruik de poorten 1812 en 1813 voor lokale RADIUS-serverwerking. In het gedeelte Default Server Priorities, definieer de standaard-EAP authenticatieprioriteit als 10.0.0.1. **Opmerking:** 10.0.0.1 is de lokale RADIUS-server.

Cisco Aironet 1300 Series Wireless Bridge

SERVER MANAGER GLOBAL PROPERTIES

Hostname bridge bridge uptime is 7 minutes

Security: Server Manager

Backup RADIUS Server

Backup RADIUS Server: (Hostname or IP Address)
 Shared Secret:

Apply Delete Cancel

Corporate Servers

Current Server List

Server: (Hostname or IP Address)
 Shared Secret:

Authentication Port (optional): (0-65536)
 Accounting Port (optional): (0-65536)

Apply Cancel

Default Server Priorities

EAP Authentication

MAC Authentication

Accounting

2. Kies **Security > Encryption Manager** in het menu links en bevestig de volgende stappen: Kies in het menu Afbeelding **AES CCMP**. Deze optie maakt AES-encryptie mogelijk met het gebruik van de Counter Mode met CBC-MAC.

Cisco Aironet 1300 Series Wireless Bridge

Hostname bridge bridge uptime is 5 minutes

Security: Encryption Manager

Encryption Modes

None

WEP Encryption

Cisco Compliant TKIP Features: Enable Message Integrity Check (MIC)
 Enable Per Packet Keying (PPK)

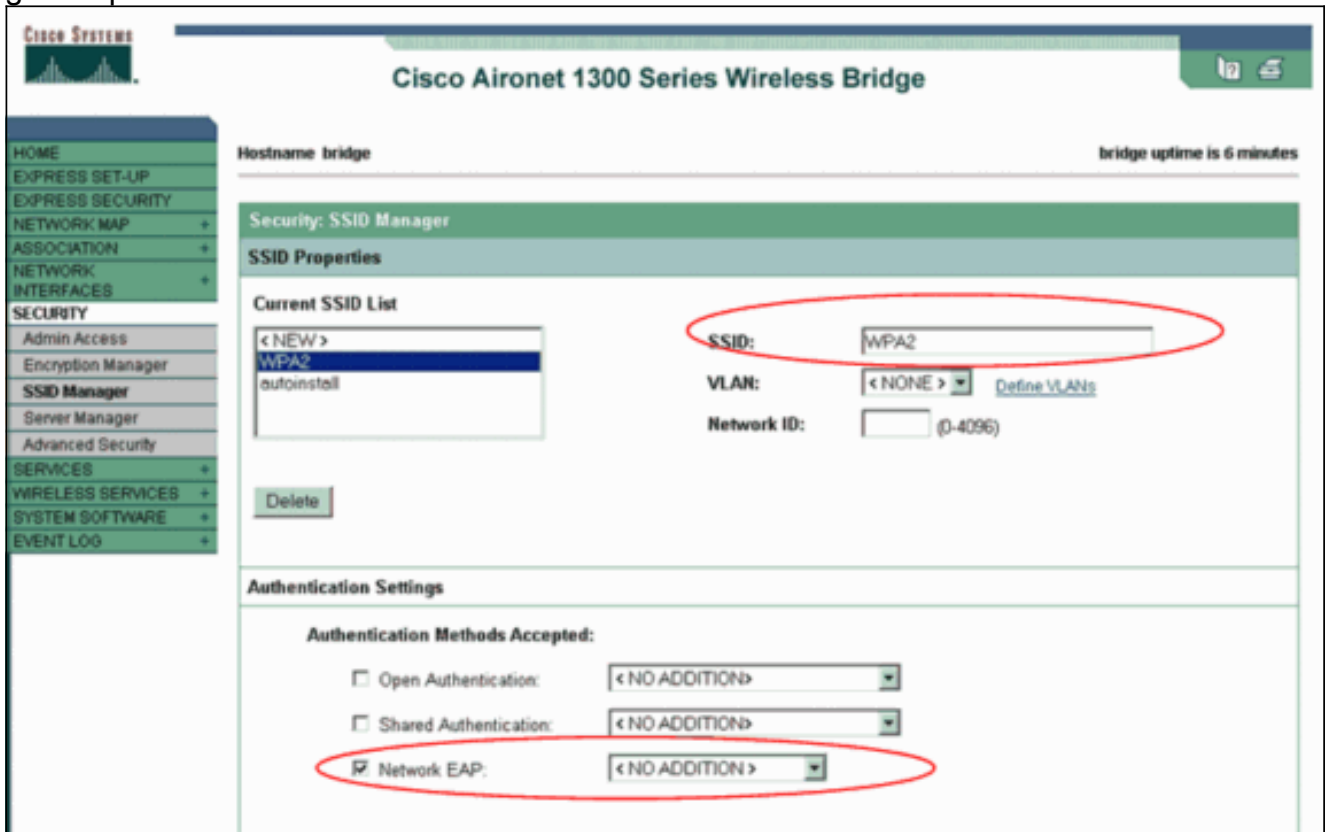
Cipher

Encryption Keys

	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 2:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	<input type="text" value="128 bit"/>

Klik op **Apply** (Toepassen).

3. Kies **Beveiliging > SSID Manager** en maak een nieuwe Service Set Identifier (SSID) voor gebruik met WAP 2. Controleer het selectieteken **EAP** in het gedeelte Verificatiemethoden geaccepteerd.



Opmerking: gebruik deze richtlijnen wanneer u het authenticatietype op de radio-interface configureren: Cisco client-gebruik MAP netwerk. Clients van derden (die Cisco-compatibele Uitbreidingen [CCX]-conforme producten omvatten)—Gebruik Open verificatie met EAP. Een combinatie van zowel Cisco als klanten van derden — Kies zowel netwerk EAP als Open Verificatie met EAP. Scroll het venster Security SSID Manager naar het gebied van Geautomatiseerde Key Management en voltooi deze stappen: Kies in het menu Key Management de optie **Verplicht**. Controleer het aanvinkvakje **WAP** rechts. Klik op **Apply** (Toepassen). **Opmerking:** de definitie van VLAN's is optioneel. Als u VLAN's definieert, worden clientapparaten die aan het gebruik van deze SSID gekoppeld zijn, in het VLAN gegroepeerd. Raadpleeg [VLAN's configureren](#) voor meer informatie over het implementeren van VLAN's.

Authenticated Key Management

Key Management: CCMP WPA

WPA Pre-shared Key: ASCII Hexadecimal

Accounting Settings

Enable Accounting

Accounting Server Priorities:

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

General Settings

Advertise Extended Capabilities of this SSID

- Advertise Wireless Provisioning Services (WPS) Support
- Advertise this SSID as a Secondary Broadcast SSID

Enable IP Redirection on this SSID

IP Address:

IP Filter (optional): [Define Filter](#)

4. Kies **Beveiliging > Local Radius Server** en vul deze stappen in: Klik op het tabblad **Algemene instelling** boven in het venster. Controleer het aanvinkvakje **LEAP** en klik op **Toepassen**. Specificeer in het gebied Netwerktoegangsservers het IP-adres en het gedeelde geheim van de RADIUS-server. Gebruik het IP-adres van het AP voor de lokale RADIUS-server.

The screenshot shows the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page is titled "Cisco Aironet 1300 Series Wireless Bridge" and has three tabs: "STATISTICS", "GENERAL SET-UP", and "EAP-FAST SET-UP". The "GENERAL SET-UP" tab is active. The page displays the following information:

- Hostname: bridge
- bridge uptime is 0 minutes
- Security: Local RADIUS Server - General Set-Up
- Local Radius Server Authentication Settings
- Enable Authentication Protocols:
 - EAP FAST
 - LEAP
 - MAC
- Network Access Servers (AAA Clients)
- Current Network Access Servers
 - < NEW >
 - 10.0.0.1
- Network Access Server: 10.0.0.1 (IP Address)
- Shared Secret: [Redacted]

Red circles highlight the "LEAP" checkbox and the "Network Access Server" and "Shared Secret" fields.

Klik op **Apply** (Toepassen).

5. Scrollt het Algemene venster voor de installatie naar het gebruikersgebied van particulieren en definieert de individuele gebruikers. De definitie van gebruikersgroepen is facultatief.

Individual Users

Current Users

<NEW>
user1

Delete

Username: user1

Password: Text NT Hash

Confirm Password:

Group Name: <NONE >

MAC Authentication Only

Apply Cancel

User Groups

Current User Groups

<NEW>

Delete

Group Name:

Session Timeout (optional): (1-4294967295 sec)

Failed Authentications before Lockout (optional): (1-4294967295)

Lockout (optional): Infinite Interval (1-4294967295 sec)

VLAN ID (optional):

SSID (optional): Add

Delete

Deze configuratie definieert een gebruiker met de naam "user1" en een wachtwoord. Bovendien selecteert de configuratie NT hash voor het wachtwoord. Na voltooiing van de procedure in deze paragraaf is de AP bereid verzoeken van cliënten om verificatie te aanvaarden. De volgende stap is de clientadapter te configureren.

CLI-configuratie

```

Access point
ap#show running-config
Building configuration...
.
.
.
aaa new-model !--- This command reinitializes the
authentication, !--- authorization and accounting
functions. !! aaa group server radius rad_eap
server 10.0.0.1 auth-port 1812 acct-port 1813
!--- A server group for RADIUS is created called
"rad_eap" !--- that uses the server at 10.0.0.1 on ports
1812 and 1813. . . . aaa authentication login
eap_methods group rad_eap
!--- Authentication [user validation] is to be done for
!--- users in a group called "eap_methods" who use
server group "rad_eap". . . . ! bridge irb ! interface

```

```

Dot11Radio0 no ip address no ip route-cache !
encryption vlan 1 key 1 size 128bit
    12345678901234567890123456 transmit-key
    !---This step is optional !--- This value seeds the
    initial key for use with !--- broadcast
    [255.255.255.255] traffic. If more than one VLAN is !---
    used, then keys must be set for each VLAN. encryption
vlan 1 mode wep mandatory
    !--- This defines the policy for the use of Wired
    Equivalent Privacy (WEP). !--- If more than one VLAN is
    used, !--- the policy must be set to mandatory for each
    VLAN. broadcast-key vlan 1 change 300
    !--- You can also enable Broadcast Key Rotation for
    each vlan and Specify the time after which Brodacst key
    is changed. If it is disabled Broadcast Key is still
    used but not changed. ssid cisco vlan 1
    !--- Create a SSID Assign a vlan to this SSID
authentication open eap eap_methods
    authentication network-eap eap_methods
    !--- Expect that users who attach to SSID "cisco" !---
    request authentication with the type 128 Open EAP and
    Network EAP authentication !--- bit set in the headers
    of those requests, and group those users into !--- a
    group called "eap_methods." ! speed basic-1.0 basic-2.0
    basic-5.5 basic-11.0 rts threshold 2312 channel 2437
    station-role root bridge-group 1 bridge-group 1
    subscriber-loop-control bridge-group 1 block-unknown-
    source no bridge-group 1 source-learning no bridge-group
    1 unicast-flooding bridge-group 1 spanning-disabled . .
    . interface FastEthernet0 no ip address no ip route-
    cache duplex auto speed auto bridge-group 1 no bridge-
    group 1 source-learning bridge-group 1 spanning-disabled
    ! interface BVI1 ip address 10.0.0.1 255.255.255.0 !---
    The address of this unit. no ip route-cache ! ip
    default-gateway 10.77.244.194 ip http server ip http
    help-path
    http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
    lp/eag/ivory/1100 ip radius source-interface BVI1 snmp-
    server community cable RO snmp-server enable traps tty
radius-server local
    !--- Engages the Local RADIUS Server feature. nas
10.0.0.1 key shared_secret
    !--- Identifies itself as a RADIUS server, reiterates !-
    -- "localness" and defines the key between the server
    (itself) and the access point(itself). ! group testuser
    !--- Groups are optional. ! user user1 nhash password1
    group testuser
    !--- Individual user user user2 nhash password2 group
    testuser
    !--- Individual user !--- These individual users
    comprise the Local Database ! radius-server host
10.0.0.1 auth-port 1812 acct-port
    1813 key shared_secret
    !--- Defines where the RADIUS server is and the key
    between !--- the access point (itself) and the server.
    radius-server retransmit 3 radius-server attribute 32
    include-in-access-req format %h radius-server
    authorization permit missing Service-Type radius-server
    vsa send accounting bridge 1 route ip ! ! line con 0
    line vty 5 15 ! end

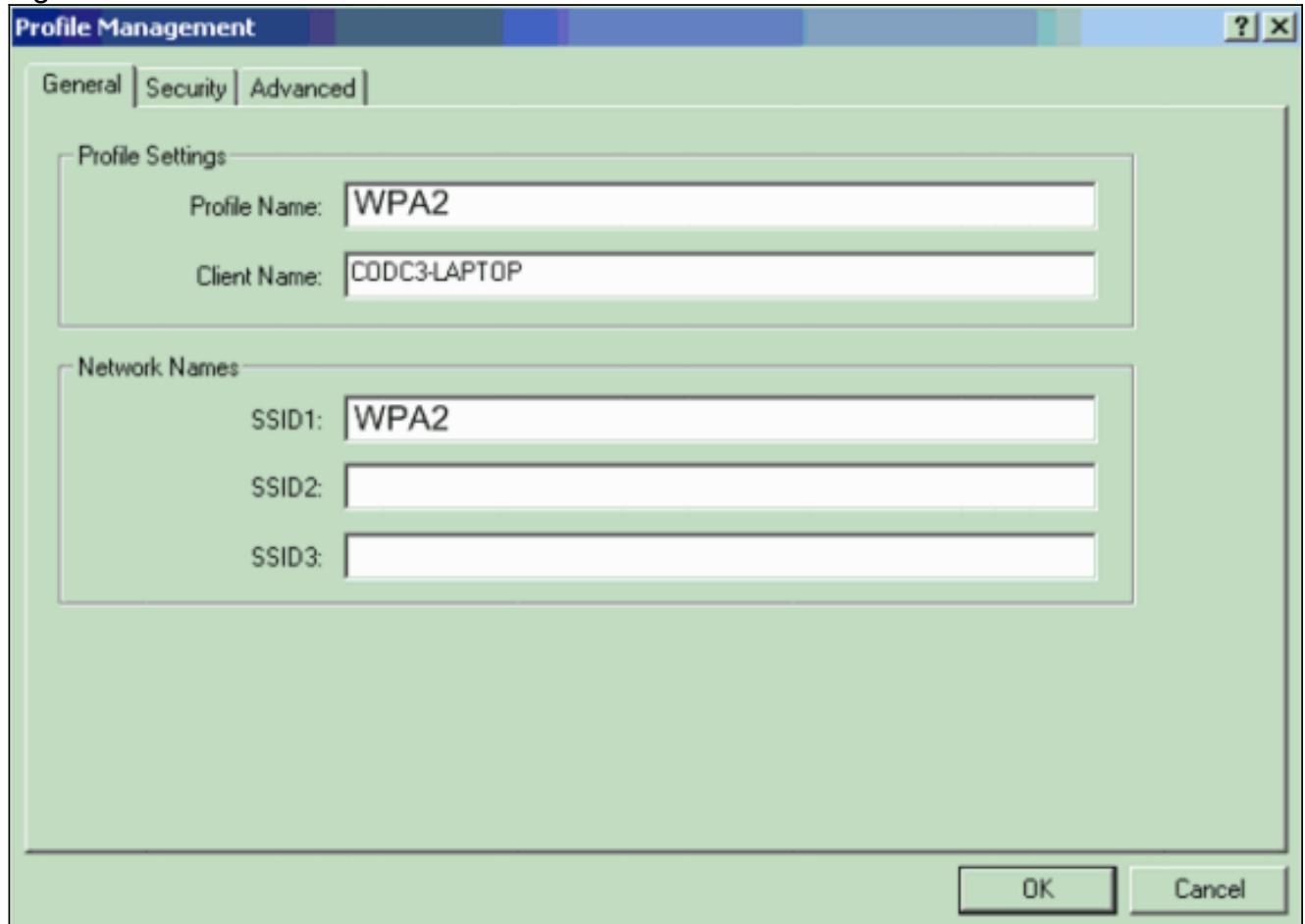
```

[De clientadapter configureren](#)

Voer de volgende stappen uit:

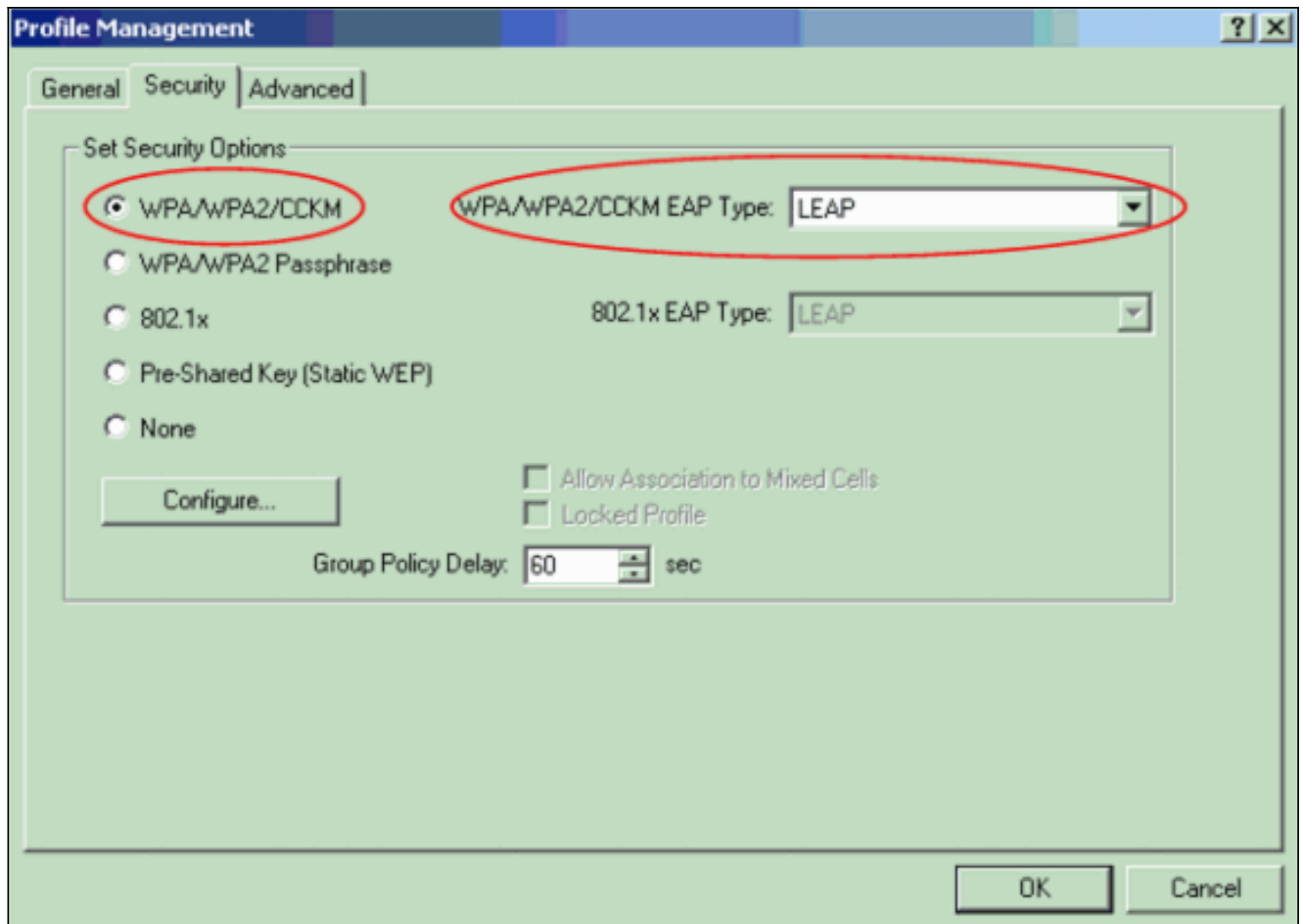
Opmerking: Dit document gebruikt een Aironet 802.11a/b/g clientadapter voor firmware 2.5 en legt de configuratie van de clientadapter uit met ADU versie 2.5.

1. Klik in het venster Profile Management op de ADU op **New** om een nieuw profiel te maken. Een nieuw venster toont waar u de configuratie voor de werking van de WAP 2-bedrijfsmodus kunt instellen. Typ onder het tabblad Algemeen de naam van het profiel en de SSID die de clientadapter zal gebruiken. In dit voorbeeld zijn de profielnaam en de SSID2: **Opmerking:** de SSID moet overeenkomen met de SSID die u op de AP voor WAP 2 hebt ingesteld.



The screenshot shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected. Under 'Profile Settings', the 'Profile Name' field contains 'WPA2' and the 'Client Name' field contains 'C0DC3-LAPTOP'. Under 'Network Names', the 'SSID1' field contains 'WPA2', while 'SSID2' and 'SSID3' are empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. Klik op het tabblad **Beveiliging**, klik op **WAP/WAP2/CCKM** en kies **LEAP** in het menu PWAP/WAP/CCKM EAP. Met deze actie kan WAP of WAP 2 worden ingesteld, welke u ook op de AP instelt.



3. Klik op **Configureren** om LEAP-instellingen te definiëren.
4. Kies de juiste naam- en wachtwoordinstellingen, gebaseerd op de vereisten, en klik op **OK**. Deze configuratie kiest de optie Automatisch oproepen voor gebruikersnaam en wachtwoord. Met deze optie kunt u de gebruikersnaam en het wachtwoord handmatig invoeren wanneer er LEAP-verificatie plaatsvindt.

LEAP Settings [?] [X]

Always Resume the Secure Session

Username and Password Settings

Use Temporary User Name and Password

Use Windows User Name and Password

Automatically Prompt for User Name and Password

Manually Prompt for User Name and Password

Use Saved User Name and Password

User Name:

Password:

Confirm Password:

Domain:

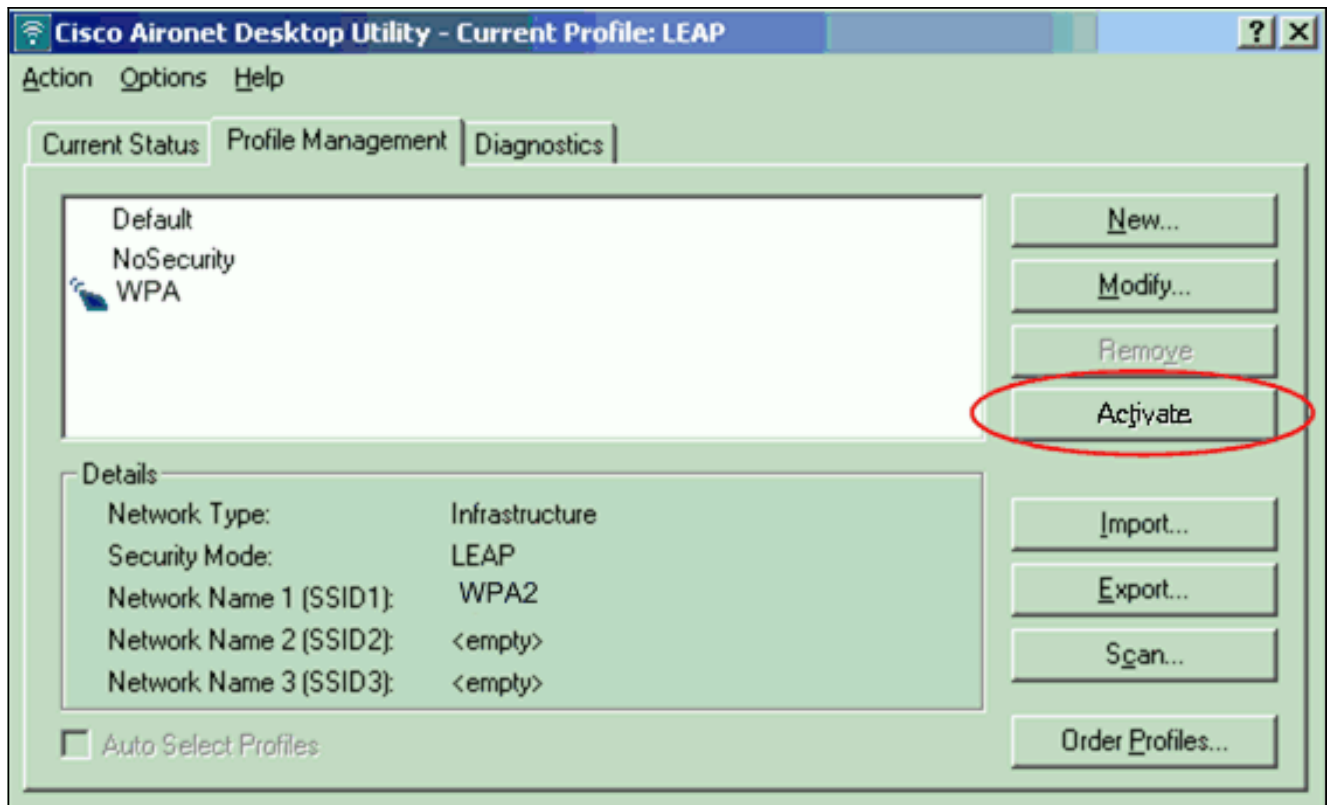
Include Windows Logon Domain with User Name

No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

5. Klik op **OK** om het venster Profile Management te sluiten.
6. Klik op **Activeren** om dit profiel op de clientadapter in te schakelen.



Opmerking: Als u Microsoft Wireless Zero Configuration (WZC) gebruikt om de clientadapter te configureren, is WPA 2 standaard niet beschikbaar bij WZC. Dus, om WZC-enabled cliënten toe te staan om WPA 2 te gebruiken, moet u een hotfix voor Microsoft Windows XP installeren. Raadpleeg het [Microsoft Download Center - Update voor Windows XP \(KB893357\)](#) voor de installatie. Nadat u de Hot Folder installeert, kunt u WPA 2 met WZC configureren.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Voer in het venster Wachtwoord voor draadloos netwerk in en voer de naam en het wachtwoord

Enter Wireless Network Password

Please enter your LEAP username and password to log on to the wireless network

User Name : user1

Password : xxxxxxx

Log on to :

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

Profile Name : WPA2

OK Cancel

in. Het volgende venster is LEAP-verificatiestatus. Deze fase verifieert de gebruikersreferenties aan de lokale RADIUS-server.

2. Controleer het statusgebied om het resultaat van de verificatie te zien.

LEAP Authentication Status

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

Profile Name: WPA2

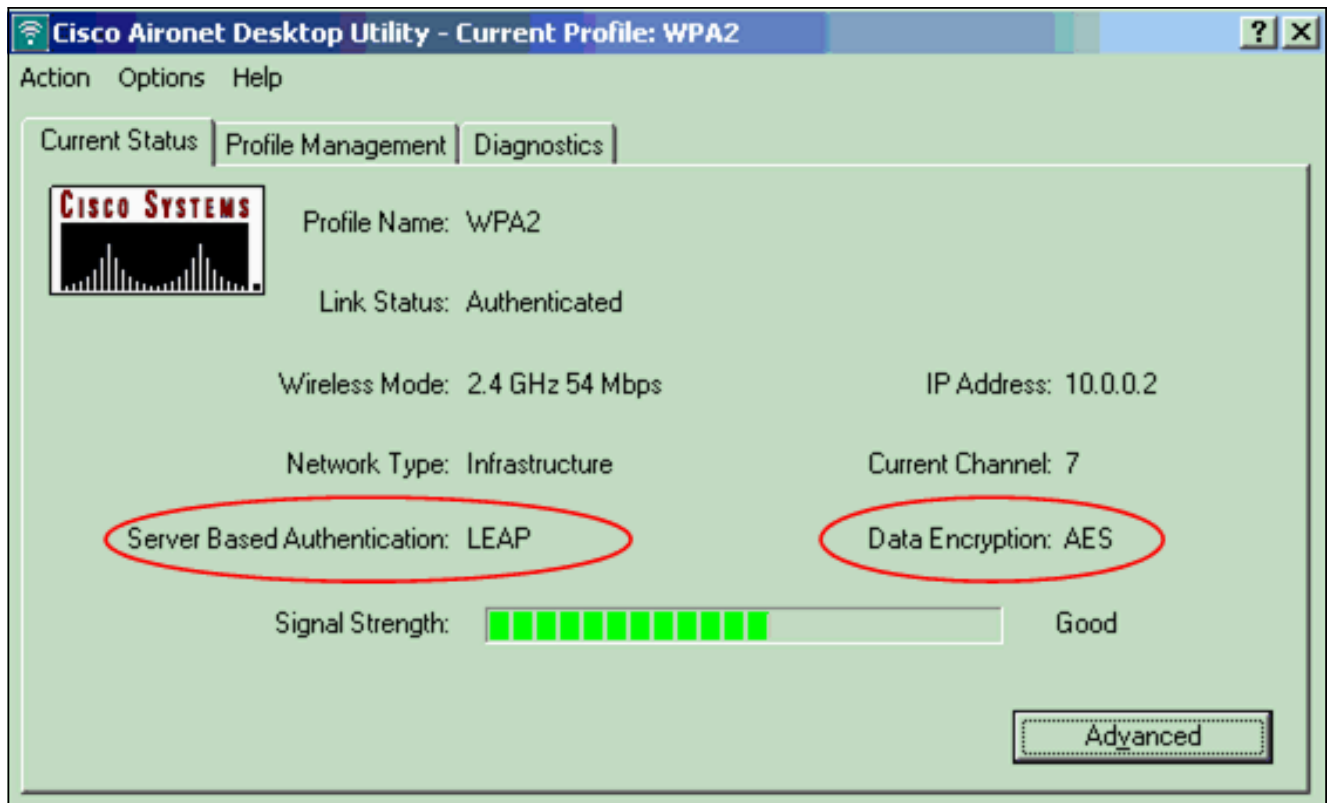
Steps	Status
1. Starting LEAP Authentication	Success
2. Checking Link Status	Success
3. Renewing IP address	Success
4. Detecting IPX Frame Type	Success
5. Finding Domain Controller	Success

Show minimized next time

Cancel

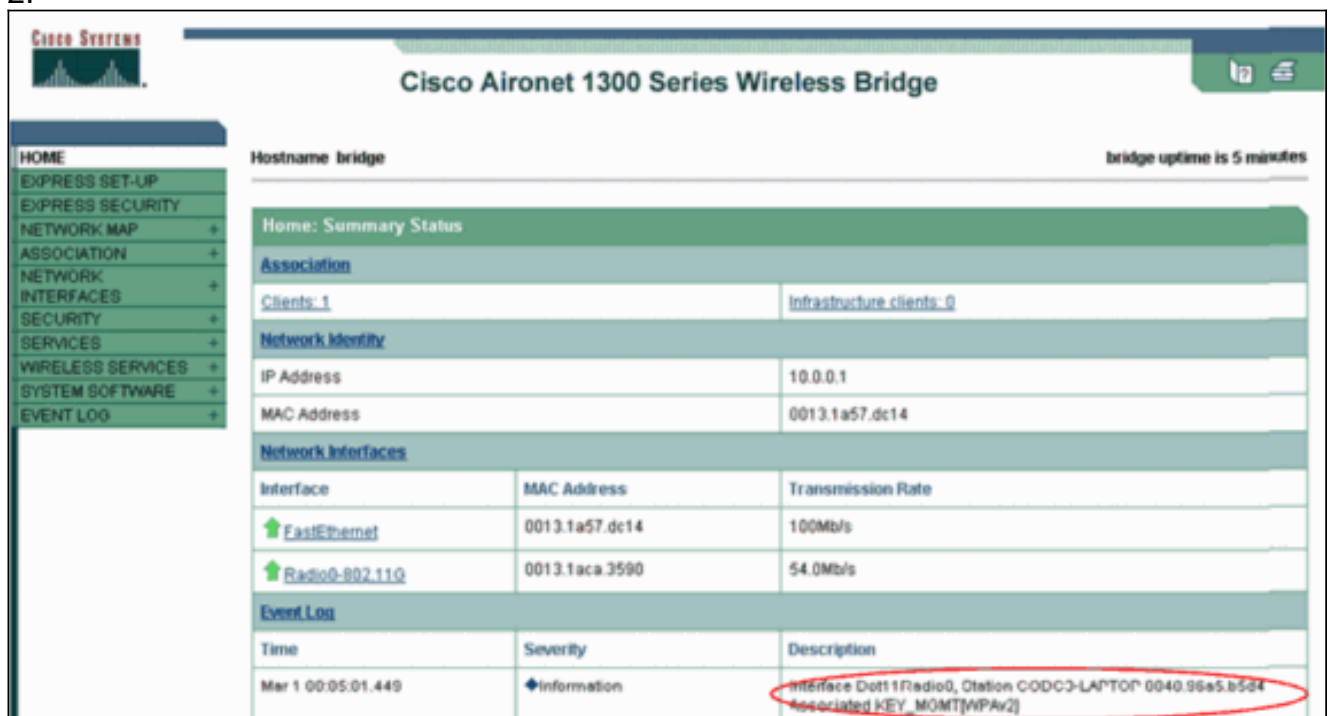
Wanneer verificatie succesvol is, sluit de client zich aan op het draadloze LAN.

3. Controleer de huidige status van de ADU om te controleren of de client AES-encryptie en LEAP-verificatie gebruikt. Dit toont aan dat u WAP 2 met MAP-verificatie en AES-encryptie in WLAN hebt geïmplementeerd.



4. Controleer het logbestand van AP/bridge Event om te controleren of de client is geauthentiseerd met WAP

2.



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Instellen in persoonlijke modus

De term **persoonlijke modus** heeft betrekking op producten die getest worden om interoperabel te zijn in de PSK-only werkwijze voor authenticatie. Voor deze modus moet er een PSK handmatig

op de AP en de clients worden ingesteld. PSK authenticereert gebruikers via een wachtwoord of identificatiecode, zowel op het clientstation als op de AP. Geen authenticatieserver is nodig. Een client heeft alleen toegang tot het netwerk als het clientwachtwoord overeenkomt met het AP-wachtwoord. Het wachtwoord voorziet ook in het sluitingsmateriaal dat TKIP of AES gebruiken om een coderingssleutel voor de encryptie van de gegevenspakketten te genereren. De persoonlijke modus is gericht op SOHO-omgevingen en wordt niet als veilig beschouwd voor ondernemingsomgevingen. Deze sectie verschaft de configuratie die u WAP 2 in de persoonlijke modus moet implementeren.

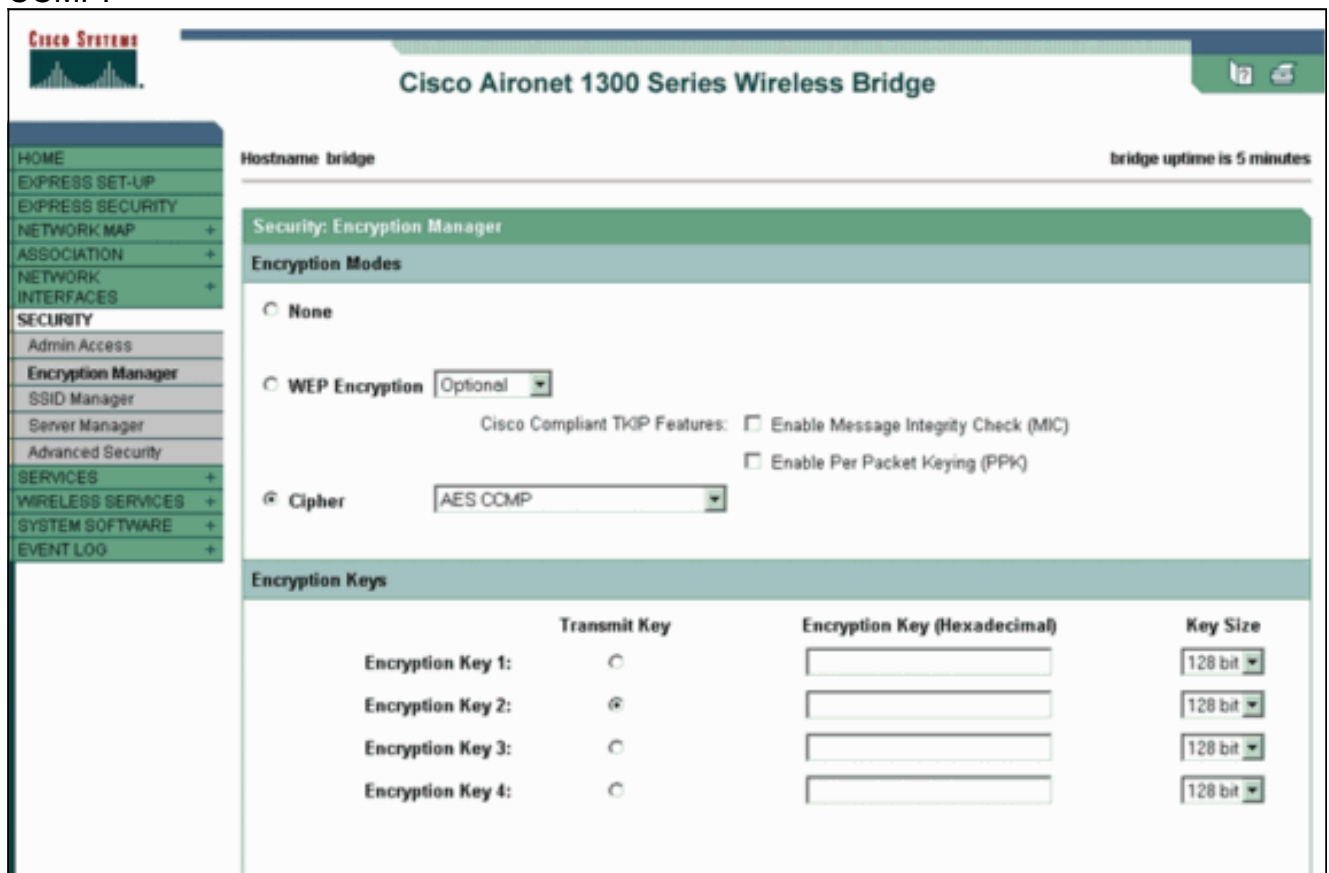
[Netwerkinstelling](#)

In deze instelling authenticereert een gebruiker met een WAP 2-compatibele clientadapter aan een Aironet 1310G AP/Bridge. Key Management vindt plaats met het gebruik van WAP 2 PSK, waarbij AES-CCMP-encryptie is geconfigureerd. De secties [Configureer de AP](#) en [configureren de clientadapter](#) tonen de configuratie op het AP en de clientadapter.

[AP configureren](#)

Voer de volgende stappen uit:

1. Kies **Security > Encryption Manager** in het menu links en voltooi deze stappen: Kies in het menu Afbeelding **AES CCMP**. Met deze optie kunt u AES-encryptie toestaan met behulp van de Counter Mode met het CCMP.



The screenshot shows the configuration page for the Cisco Aironet 1300 Series Wireless Bridge, specifically the Security: Encryption Manager section. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The bridge uptime is 5 minutes. The left sidebar contains a navigation menu with options like HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, Admin Access, Encryption Manager, SSID Manager, Server Manager, Advanced Security, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Security: Encryption Manager" and "Encryption Modes". Under "Encryption Modes", there are three radio buttons: "None", "WEP Encryption" (with a dropdown menu set to "Optional"), and "Cipher" (which is selected). Below "Cipher", there is a dropdown menu set to "AES CCMP". There are also two checkboxes for "Cisco Compliant TKIP Features": "Enable Message Integrity Check (MIC)" and "Enable Per Packet Keying (PPK)". Below this, there is a section titled "Encryption Keys" with a table for configuring keys.

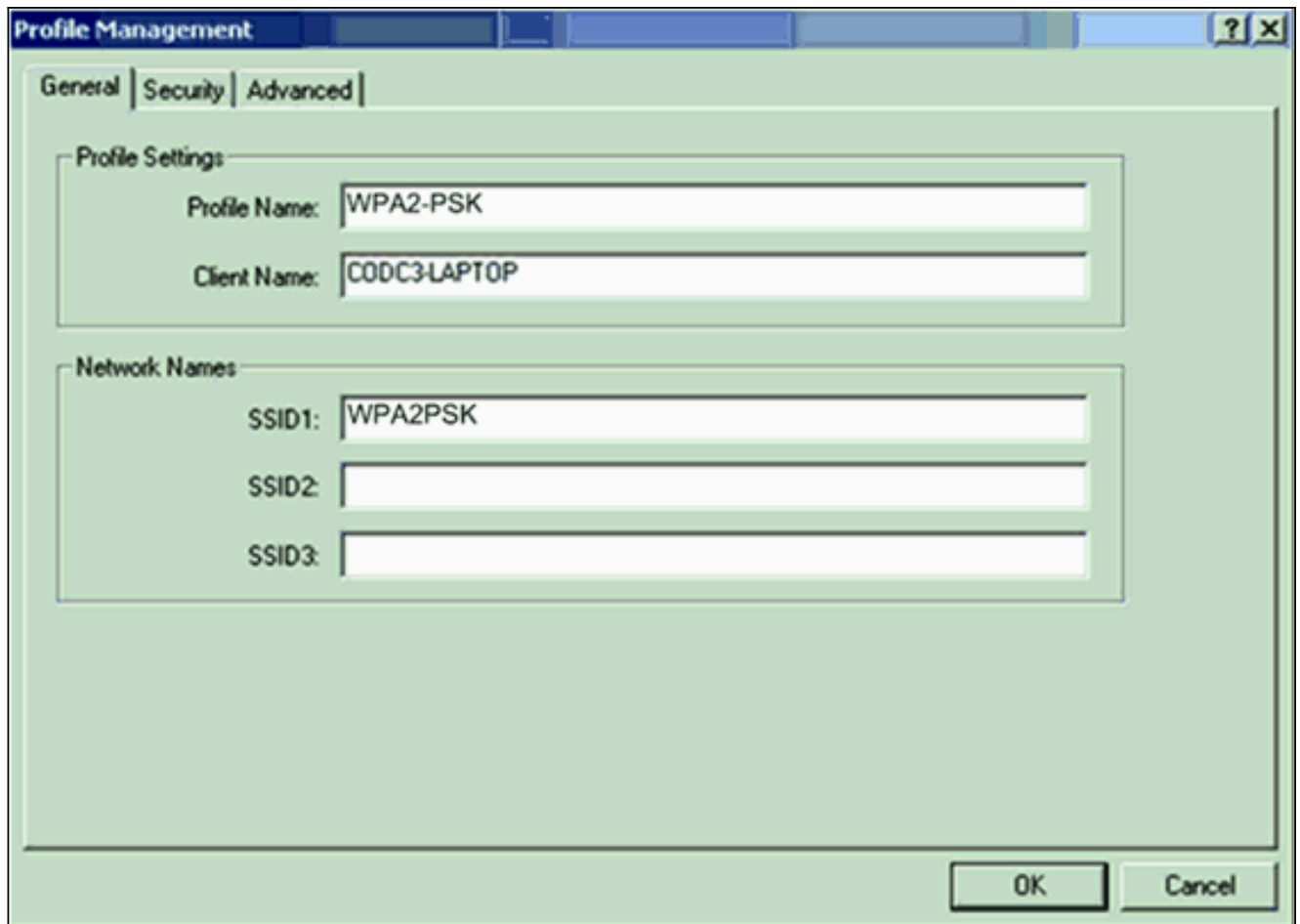
	Transmit Key	Encryption Key (Hexadecimal)	Key Size
Encryption Key 1:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 2:	<input checked="" type="radio"/>	<input type="text"/>	128 bit
Encryption Key 3:	<input type="radio"/>	<input type="text"/>	128 bit
Encryption Key 4:	<input type="radio"/>	<input type="text"/>	128 bit

Klik op **Apply** (Toepassen).

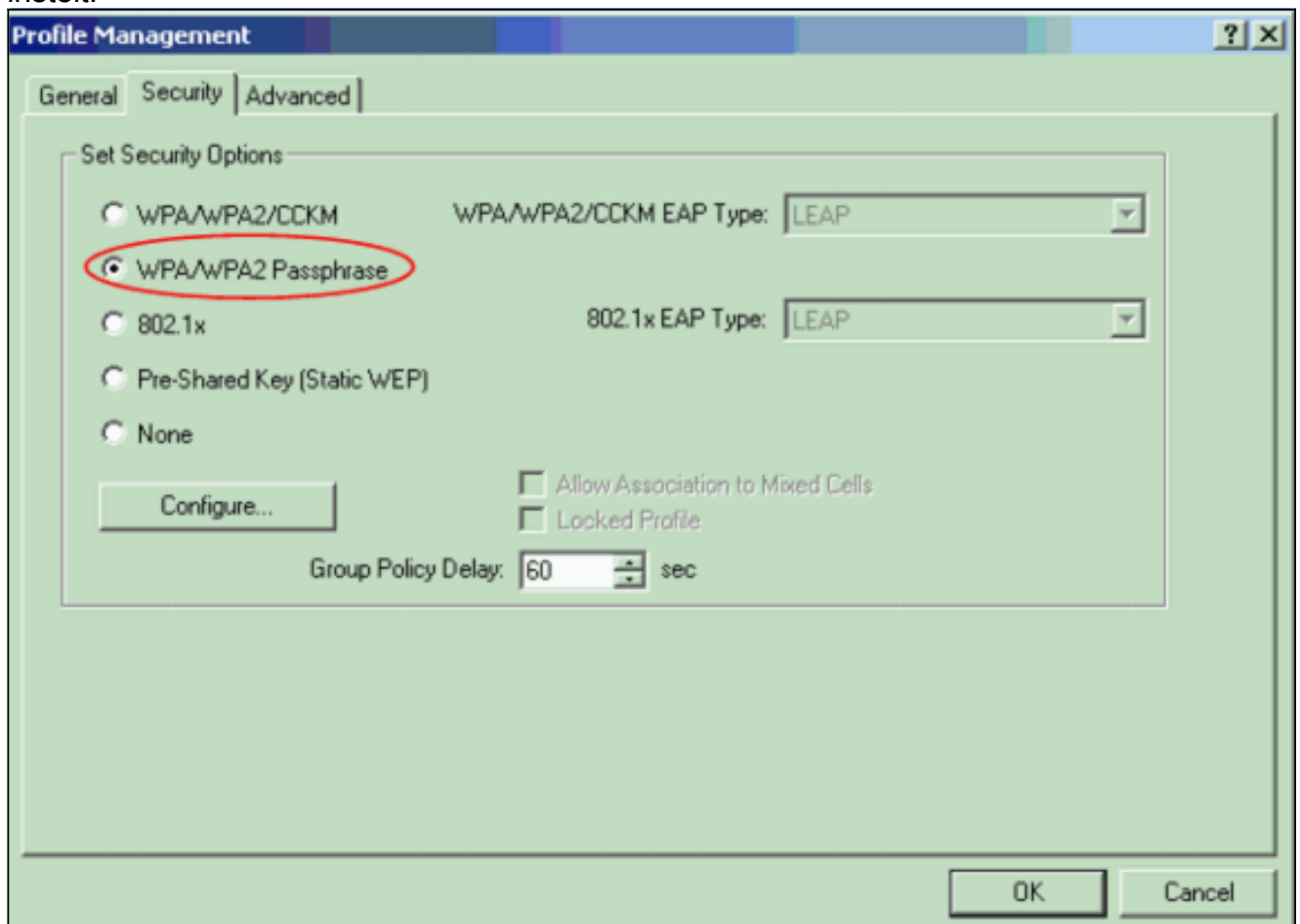
2. Kies **Beveiliging > SSID Manager** en maak een nieuwe SSID voor gebruik met WAP
2. Controleer het vakje **Open Verificatie**.

The screenshot displays the configuration interface for a Cisco Aironet 1300 Series Wireless Bridge. The page title is "Cisco Aironet 1300 Series Wireless Bridge" and the hostname is "bridge". The bridge uptime is 7 minutes. The left sidebar shows the navigation menu with "SSID Manager" selected under the "SECURITY" section. The main content area is titled "Security: SSID Manager" and "SSID Properties". It shows a "Current SSID List" with a table containing a "NEW" entry and "WPA2PSK" (selected) and "tsunami". To the right, the "SSID:" field is set to "WPA2PSK", "VLAN:" is set to "< NONE >", and "Network ID:" is empty. Below this, the "Authentication Settings" section shows "Authentication Methods Accepted:" with "Open Authentication" checked and "Shared Authentication" and "Network EAP" unchecked. Red circles highlight the "WPA2PSK" SSID and the "Open Authentication" checkbox.

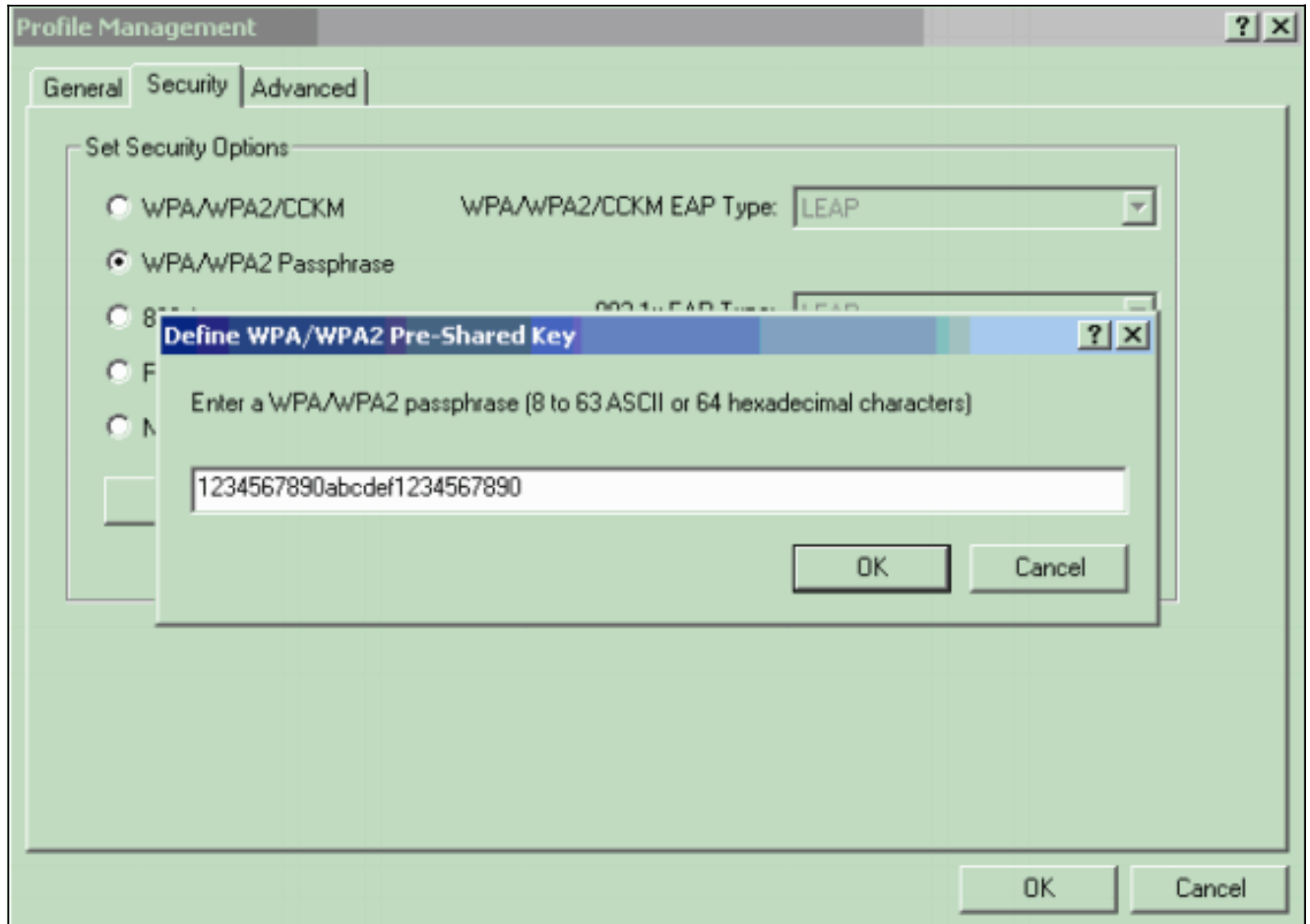
Scroll door de beveiliging: Het venster van SSID Manager aan het gebied van Geautomatiseerde Key Management en voltooi deze stappen: Kies in het menu Key Management de optie **Verplicht**. Controleer het aanvinkvakje **WAP** rechts.



2. Klik op het tabblad **Beveiliging** en klik op het tabblad **WAP/WAP2-wachtwoord**. Met deze actie kan WAP PSK of WAP 2 PSK worden ingesteld, welke u ook op de AP instelt.



3. Klik op **Configureren**. Vooraf gedeelde venster van de sleutel van het venster Definieer WAP/WAP2.
4. Verkrijg het wachtwoord van WAP/WAP2 van uw systeembeheerder en voer het wachtwoord in het veld Wachtwoord van WAP/WAP2 in. Verkrijg het wachtwoord voor AP in een infrastructuurnetwerk of het wachtwoord voor andere klanten in een ad hoc netwerk. Gebruik deze richtlijnen om een wachtwoord in te voeren: WAP/WAP2-wachtrijen moeten tussen 8 en 63 ASCII-teksttekens of 64 hexadecimale tekens bevatten. Het wachtwoord van de client-WAP/WAP2 moet overeenkomen met het wachtwoord van de AP waarmee u wilt communiceren.



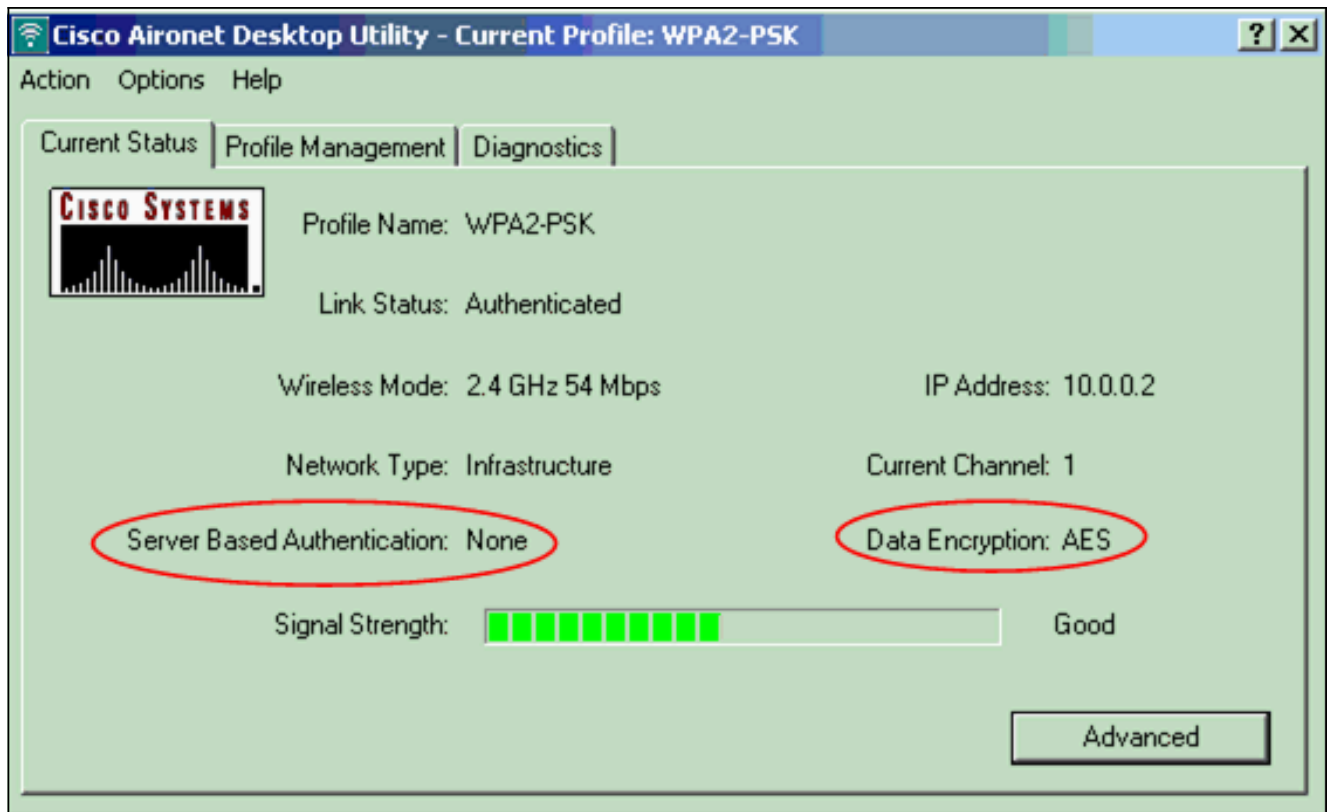
5. Klik op **OK** om het wachtwoord op te slaan en terug te keren naar het venster Profile Management.

Verifiëren

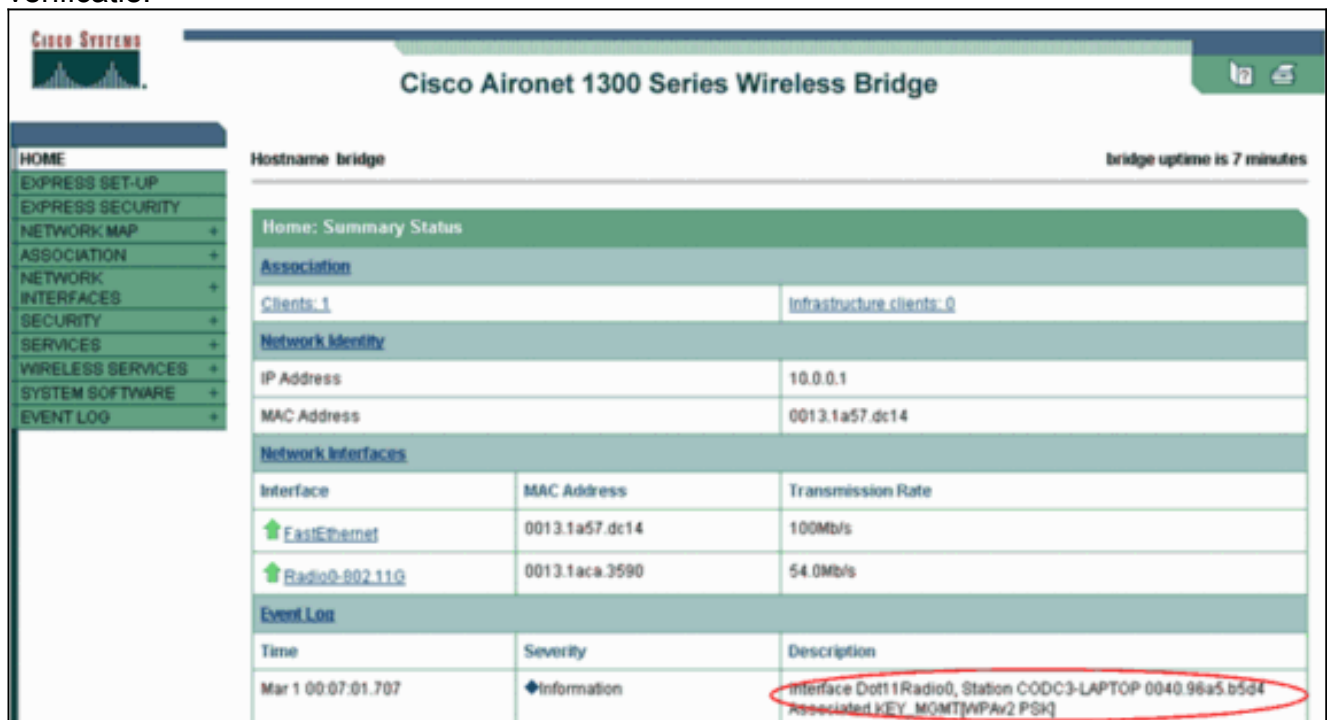
Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Nadat het WAP 2 PSK-profiel is geactiveerd, authenticceert de AP de client op basis van het WAP 2-wachtwoord (PSK) en geeft deze toegang tot het WLAN.

1. Controleer de huidige status van de ADU om succesvolle verificatie te controleren. Dit venster geeft een voorbeeld. Het venster toont aan dat de gebruikte encryptie AES is en dat geen op een server gebaseerde authenticatie wordt uitgevoerd:



2. Controleer het logbestand van AP/bridge Event om te controleren of de client is geauthentiseerd met WAP 2 PSK-modus van verificatie.



Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Cipuites en EFN configureren](#)

- [Verificatietypen configureren](#)
- [Overzicht van WAP-configuratie](#)
- [WAP2 - Wi-Fi beschermde toegang 2](#)
- [Wat is de gemengde werking van WAP en hoe vorm ik het in mijn AP](#)
- [Draadloze ondersteuningspagina](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)