

Draadloze verificatietypen op een vaste ISR configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Open verificatie configureren](#)

[Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)

[De overbrugde virtuele interface configureren \(BVI\)](#)

[Configuratie van SSID voor Open Verificatie](#)

[Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN 802.1x/EAP-verificatie configureren](#)

[Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)

[De overbrugde virtuele interface configureren \(BVI\)](#)

[De lokale RADIUS-server voor EAP-verificatie configureren](#)

[De SSID's configureren voor 802.1x/EAP-verificatie](#)

[Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

[WAP-toepassingsbeheer](#)

[WAP-PSK configureren](#)

[Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)

[De overbrugde virtuele interface configureren \(BVI\)](#)

[Configureer de SSID's voor WAP-PSK-verificatie](#)

[Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

[WAP-verificatie configureren \(met EAP-verificatie\)](#)

[Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)

[De overbrugde virtuele interface configureren \(BVI\)](#)

[De lokale RADIUS-server voor WAP-verificatie configureren](#)

[SSID voor WAP configureren met EAP-verificatie](#)

[Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

[Draadloze client voor verificatie configureren](#)

[De draadloze client voor Open Verificatie configureren](#)

[De draadloze client configureren voor 802.1x/EAP-verificatie](#)

[De draadloze client voor WAP-PSK-verificatie configureren](#)

[De draadloze client voor WAP configureren \(met EAP\)](#)

[Problemen oplossen](#)

[Opdrachten voor troubleshooting](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document biedt een configuratievoorbeeld dat uitlegt hoe u verschillende Layer 2-authenticatietypen kunt configureren op een Cisco draadloze geïntegreerde configuratie-router voor draadloze connectiviteit met CLI-opdrachten.

[Voorwaarden](#)

[Vereisten](#)

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

- Kennis van hoe u de basisparameters van Cisco geïntegreerde services router (ISR) kunt configureren
- Kennis van de manier waarop u de 802.11a/b/g draadloze clientadapter kunt configureren met het Aironet-desktohpulprogramma (ADU)

[Gebruikte componenten](#)

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

- Cisco 877W ISR-software voor Cisco IOS-software-release 12.3(8)Y11
- Laptop met Aironet desktohpulprogramma versie 3.6
- 802.11a/b/g clientadapter voor firmware versie 3.6

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 de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

[Achtergrondinformatie](#)

De Cisco geïntegreerde services routers voor vaste configuratie ondersteunen een beveiligde, betaalbare en makkelijk te gebruiken draadloze LAN-oplossing die mobiliteit en flexibiliteit combineert met de functies op bedrijfsniveau die vereist zijn door netwerkprofessionals. Met een beheersysteem dat is gebaseerd op Cisco IOS-software, fungeren de Cisco-routers als access points en zijn Wi-Fi gecertificeerd: IEEE 802.11a/b/g-conforme draadloze LAN-transceivers.

U kunt de routers configureren en bewaken met de opdrachtregel-interface (CLI), het op browser gebaseerde beheersysteem of Simple Network Management Protocol (SNMP). Dit document

beschrijft hoe u de ISR voor draadloze connectiviteit met de CLI-opdrachten kunt configureren.

Configureren

Dit voorbeeld toont hoe te om deze authenticatietypen op een Cisco Draadloze Geïntegreerde configuratierouter met CLI opdrachten te configureren.

- Open authenticatie
- 802.1x/EAP (Extensible Authentication Protocol)-verificatie
- Wi-Fi vooraf gedeelde sleutel (WAP-PSK) voor beveiligde toegang
- WPP-verificatie (met MAP)

Opmerking: Dit document is niet gericht op gedeelde authenticatie aangezien het een minder beveiligd authenticatietype is.

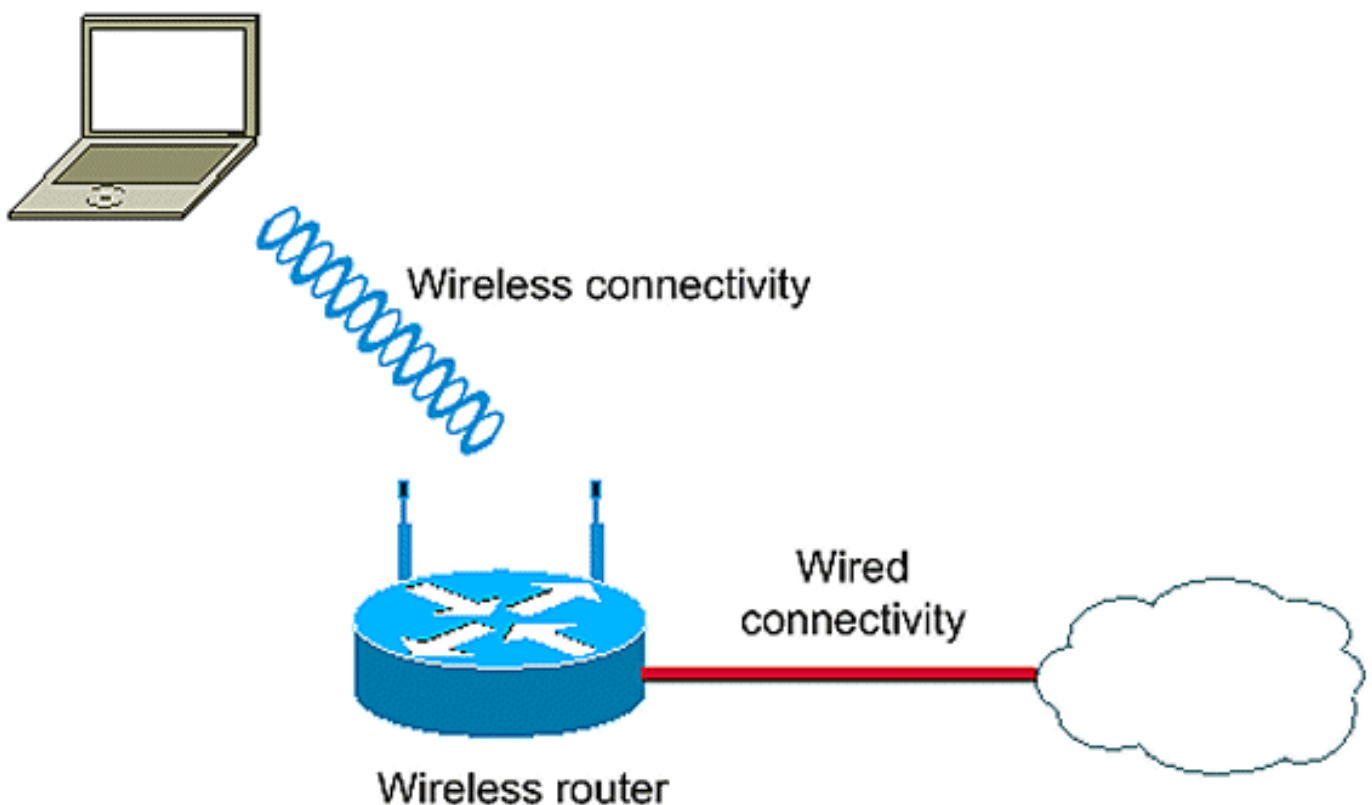
Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het [Opname Gereedschap](#) ([alleen geregistreerde](#) klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:

Wireless LAN Client



Deze instelling gebruikt de lokale RADIUS-server op de draadloze ISR om draadloze klanten met 802.1x-verificatie voor eensluidend te verklaren.

Open verificatie configureren

Open authenticatie is een ongeldig authenticatiealgoritme. Het toegangspunt verleent elk verzoek om echtheidscontrole. Open authenticatie maakt elke netwerktoegang voor apparaten mogelijk. Als geen encryptie op het netwerk is ingeschakeld, kan elk apparaat dat de SSID van het access point kent, toegang tot het netwerk krijgen. Als de encryptie van EFG op een toegangspunt wordt geactiveerd, wordt de sleutel van de EVN zelf een middel van toegangscontrole. Als een apparaat niet de juiste sleutel van EFG heeft, zelfs al is de authenticatie succesvol, kan het apparaat geen gegevens door het toegangspunt verzenden. En het kan ook geen gegevens decrypteren die van het toegangspunt verstuurd worden.

Deze voorbeeldconfiguratie verklaart alleen een eenvoudige open authenticatie. De de sleutel van de EVN kan verplicht of facultatief worden gemaakt. Dit voorbeeld vormt de sleutel van EFG als optioneel zodat elk apparaat dat geen gebruik maakt van EFG ook voor authentiek kan zijn en met deze AP kan associëren.

Raadpleeg [Open verificatie](#) voor meer informatie.

Dit voorbeeld gebruikt deze configuratie instellingen om open authenticatie op ISR te configureren.

- SSID-naam: "open"
- VLAN 1
- Interne DHCP-serverbereik: 10.1.0.0/16

Opmerking: Ter wille van de eenvoud gebruikt dit voorbeeld geen encryptietechniek voor geauthentiseerde klanten.

Voltooi deze acties op de router:

1. [Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)
2. [De overbrugde virtuele interface configureren \(BVI\)](#)
3. [Configuratie van SSID voor Open Verificatie](#)
4. [Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

Het geïntegreerde routing en bridging (IRB) configureren en de Bridge Group instellen

Voltooi deze acties:

1. **Schakel IRB in de router in.**`router<configuratie>#bridge irb`**Opmerking:** Als alle security typen op één router ingesteld moeten worden, is deze voldoende om IRB slechts eenmaal mondiaal op de router mogelijk te maken. Het hoeft niet voor elk afzonderlijk authenticatietype te worden ingeschakeld.
2. **Definieer een bruggroep.**Dit voorbeeld gebruikt het bridge-group nummer `1`.`router<configuratie>#bridge 1`
3. **Kies het overspannen van een boomprotocol voor de bridge groep.**Hier wordt het IEEE die boomprotocol omspant voor deze bridge groep geconfigureerd.`router<configuratie>#bridge 1 protocol-ieee`
4. **Laat een BVI toe om routeerbare pakketten die van zijn correspondent bridge groep worden ontvangen en te leiden.**Dit voorbeeld stelt de BVI in staat het IP-pakket te aanvaarden en te

verzenden.router<configuratie>**#bridge 1 route-ip**

De overbrugde virtuele interface configureren (BVI)

Voltooi deze acties:

1. **Configureer de BVI.**Configureer de BVI wanneer u het corresponderende nummer van de bruggroep aan de BVI toewijst. Elke overbruggingsgroep kan slechts één overeenkomend BVI hebben. Dit voorbeeld wijst bridge group nummer 1 toe aan de BVI.router<configuratie>**#interface BVI <1>**
2. **Geef een IP-adres aan de BVI toe.**router<span-if>**#ip-adres 10.1.1.1 255.255.0.0**router<span-if>**#no afgesloten**

Raadpleeg [Overbrugging configureren](#) voor gedetailleerde informatie over overbrugging.

Configuratie van SSID voor Open Verificatie

Voltooi deze acties:

1. **Schakel de radio-interface in**Ga naar de configuratie-modus van de DOT11-radio om de interface te activeren en wijs een SSID aan de interface toe.router**#interface-punt11radio0**router<span-if>**#no shutdown**router<Config-if>**#ssid open**Het open authenticatietype kan in combinatie met MAC-adresverificatie worden ingesteld. In dit geval, dwingt het toegangspunt alle clientapparaten om MAC-adresverificatie uit te voeren voordat ze zich bij het netwerk mogen aansluiten.Open authenticatie kan ook samen met MAP-authenticatie worden ingesteld. Het toegangspunt dwingt alle clientapparaten om MAP-authenticatie uit te voeren voordat ze zich bij het netwerk mogen aansluiten. Specificeer voor de lijst-naam de lijst met de verificatiemethode.Een toegangspunt dat is ingesteld voor MAP-authenticatie dwingt alle clientapparaten die geassocieerd zijn met het uitvoeren van MAP-authenticatie. Clientapparaten die geen MAP gebruiken, kunnen het toegangspunt niet gebruiken.
2. **Bind SSID aan een VLAN.**Om SSID op deze interface in te schakelen, bindt SSID aan het VLAN in de configuratie van SSID.router<span-ssid>**VLAN 1**
3. **Configureer de SSID met open verificatie.**router<span-ssid>**#authenticatie open**
4. **Configureer de radio-interface voor de EFN-toets optioneel.**router<Configuration>**#encryptie VLAN 1-modus**
5. **Schakel VLAN in op de radio-interface.**router**#interface Dot11Radio 0.1**router<span-subif>**#encapsulation dot1Q 1**router<span-subif>**#bridge-group 1**

Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN

Typ deze opdrachten in de configuratie-modus wereldwijd om de interne DHCP-server voor de draadloze clients van dit VLAN te configureren:

- **ip dhcp exclusief adres 10.1.1.1 10.1.1.5**
- **ip - dhcp - pool open**

Typ in de DHCP-podconfiguratie deze opdrachten:

- netwerk *10.1.0.0 255.255.0.0*
- Standaard-router *10.1.1.1*

802.1x/EAP-verificatie configureren

Dit authenticatietype biedt het hoogste veiligheidsniveau voor uw draadloos netwerk. Aangezien het Extensible Authentication Protocol (EAP) wordt gebruikt om te interacteren met een EAP-compatibele RADIUS-server, helpt het toegangspunt een draadloos client-apparaat en de RADIUS-server om wederzijdse authenticatie uit te voeren en een dynamische Toerichte eensnelheids-sleutel af te leiden. De RADIUS-server verstuurt de sleutel van EFN naar het toegangspunt, dat het gebruikt voor alle unicast-gegevenssignalen die het van de client verstuurt of ontvangt.

Raadpleeg [EAP-verificatie](#) voor meer informatie.

Dit voorbeeld gebruikt deze configuratie instellingen:

- SSID-naam: **sprong**
- VLAN 2
- Interne DHCP-serverbereik: **10.2.0.0/16**

In dit voorbeeld wordt gebruik gemaakt van LEAP-authenticatie als het mechanisme om de draadloze client te authenticeren.

Opmerking: Raadpleeg [Cisco Secure ACS voor Windows v3.2 met EAP-TLS Machine-verificatie](#) om EAP-TLS te configureren.

Opmerking: Raadpleeg [Cisco Secure ACS voor Windows v3.2 configureren met PEAP-MS-CHAPv2-machineverificatie](#) om PEAP-MS-CHAPv2 te configureren.

Toelichting: Begrijp dat alle configuratie van deze MAP-typen hoofdzakelijk betrekking heeft op de configuratie van de klant en de authenticatieserver. De configuratie op de draadloze router of het access point blijft min of meer hetzelfde voor al deze authenticatietypen.

Opmerking: Zoals eerder vermeld, gebruikt deze instelling de lokale RADIUS-server op de draadloze ISR om draadloze klanten met 802.1x-verificatie voor eensluidend te verklaren.

Voltooi deze acties op de router:

1. [Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)
2. [De overbrugde virtuele interface configureren \(BVI\)](#)
3. [De lokale RADIUS-server voor EAP-verificatie configureren](#)
4. [De SSID's configureren voor 802.1x/EAP-verificatie](#)
5. [Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

Het geïntegreerde routing en bridging (IRB) configureren en de Bridge Group instellen

Voltooi deze acties:

1. **Schakel IRB in de router in.**router<configuratie>#bridge irb**Opmerking:** Als alle security typen

op één router ingesteld moeten worden, is deze voldoende om IRB slechts eenmaal mondiaal op de router mogelijk te maken. Het hoeft niet voor elk afzonderlijk authenticatietype te worden ingeschakeld.

2. **Definieer een bruggroep.**Dit voorbeeld gebruikt het bridge-group nummer 2.
`router<configuratie>#bridge 2`
3. **Kies het overspannen van een boomprotocol voor de bridge groep.**Hier wordt het IEEE die in een boom protocol omspant voor deze bridge groep geconfigureerd.
`router<configuratie>#bridge 2 protocol-ieee`
4. **Kies het overspannen van een boomprotocol voor de bridge groep.**Hier wordt het IEEE die in een boom protocol omspant voor deze bridge groep geconfigureerd.
`router<configuratie>#bridge 2 protocol-ieee`
5. **Schakel een BVI in om routekaarten te aanvaarden en te routeren die van zijn corresponderende bridge groep worden ontvangen.**Dit voorbeeld stelt de BVI in staat IP-pakketten te aanvaarden en te verzenden.
`router<configuratie>#bridge 2 route-ip`

[De overbrugde virtuele interface configureren \(BVI\)](#)

Voltooi deze acties:

1. **Configureer de BVI.**Configureer de BVI wanneer u het corresponderende nummer van de bruggroep aan de BVI toewijst. Elke overbruggingsgroep kan slechts één correspondent BVI hebben. Dit voorbeeld kent bridge group nummer 2 toe aan de BVI.
`router<configuratie>#interface BVI <2>`
2. **Geef een IP-adres aan de BVI toe.**
`router<span-if>#ip-adres 10.2.1.1 255.255.0.0`
`router<span-if>#no afgesloten`

[De lokale RADIUS-server voor EAP-verificatie configureren](#)

Zoals eerder vermeld, gebruikt dit document lokale RADIUS-server op de draadloze bewuste router voor MAP-verificatie.

1. **Schakel het controlemodel voor verificatie, autorisatie en accounting (AAA) in.**
`router<configuratie>#aaa nieuw-model`
2. **Maak een servergroep doorsturen voor de RADIUS-server.**
`router<Configuration>#aaa group server Straal -eap server 10.2.1.1 auth-Port 1812 poort 1813`
3. **Maak een methode lijst eap_methods die de authenticatiemethode aangeeft die wordt gebruikt om de AAA login gebruiker te authenticeren.** Pas de methodelijst toe aan deze servergroep.
`router<configuratie>#aaa authenticatie inloggen eap_methods groep rad-eap`
4. **Schakel de router in als een lokale authenticatieserver en voer de configuratiemodus in voor de authenticator.**
`router<configuratie>#Straal-server lokaal`
5. **In de configuratiemodus voor Radius Server kunt u de router als een AAA-client voor de lokale verificatieserver toevoegen.**
`router<span-rv>#nas 10.2.1.1 toets Cisco`
6. **Configureer gebruiker user1 op de lokale RADIUS-server.**
`router<Configuration-radsrv>#user user1 wachtwoord user1 group rad-eap`
7. **Specificeer de RADIUS-serverhost.**
`router<span-radsrv>#Straal-server host 10.2.1.1 augustus-poorts 1812 ACT-poort 1813 cisco-toets`
Opmerking: Deze toets moet gelijk zijn aan de toets die is gespecificeerd in nas-opdracht onder de Straal-Server configuratie modus.

De SSID's configureren voor 802.1x/EAP-verificatie

De configuratie van de radio-interface en de bijbehorende SSID's voor 802.1x/EAP omvat de configuratie van verschillende draadloze parameters op de router, die de SSID, de coderingsmodus en het authenticatietype omvat. Dit voorbeeld gebruikt SSID genoemd *leap*.

1. **Schakel de radio-interface in.** Ga naar de configuratie-modus van de DOT11-radiointerface om de radio-interface te activeren en wijs een SSID aan de interface toe.
router#interface-punt11radio0router<span-if>#no shutdownrouter<Config-if>#ssid *leap*
2. **Bind SSID aan een VLAN.** Om SSID op deze interface in te schakelen, bindt SSID aan het VLAN in de configuratie van SSID.
router<span-ssid>#vlan 2
3. **Configureer de SSID met 802.1x/LEAP-verificatie.**
router<span-ssid>#Authentication-netwerk-eap *eap_methods*
4. **Configureer de radio-interface voor dynamisch sleutelbeheer.**
router#encryptie VLAN 2 mode-ciphers wep40
5. **Schakel VLAN in op de radio-interface.**
router#interface Dot11Radio 0.2router<span-subif>#encapsulation dot1Q 2router<span-subif>#bridge-group 2

Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN

Typ deze opdrachten in de configuratie-modus wereldwijd om de interne DHCP-server voor de draadloze clients van dit VLAN te configureren:

- ip dhcp exclusief adres 10.2.1.1 10.2.1.5
- ip dhcp pool *leapauth*

Typ in de DHCP-podconfiguratie deze opdrachten:

- netwerk 10.2.0.0 255.255.0.0
- Standaard-router 10.2.1.1

WAP-toepassingsbeheer

Wi-Fi Protected Access is een op standaarden gebaseerde, interoperabele beveiligingsverbetering die het niveau van gegevensbescherming en toegangscontrole voor huidige en toekomstige draadloze LAN-systemen sterk verhoogt.

Raadpleeg [WAP](#)-sleutelbeheer voor meer informatie.

WAP-sleutelbeheer ondersteunt twee elkaar uitsluitende beheertypen: WAP-Pre-Sgedeeld sleutel (WAP-PSK) en WAP (met EAP).

WAP-PSK configureren

WAP-PSK wordt gebruikt als een beheertype dat van essentieel belang is voor een draadloos LAN waarin 802.1x-gebaseerde verificatie niet beschikbaar is. In dergelijke netwerken moet u een vooraf gedeelde toets op het toegangspunt configureren. U kunt de vooraf gedeelde toets als

ASCII of hexadecimale tekens invoeren. Als u de toets als ASCII-tekens invoert, voert u 8 tot 63 tekens in en het access point breidt de toets uit met het proces dat is beschreven in de Password-Based Cryptography Standard (RFC2898). Als u de toets als hexadecimale tekens invoert, moet u 64 hexadecimale tekens invoeren.

Dit voorbeeld gebruikt deze configuratie instellingen:

- SSID-naam: **gedeeld**
- VLAN 3
- Interne DHCP-serverbereik: **10.3.0.0/16**

Voltooi deze acties op de router:

1. [Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)
2. [De overbrugde virtuele interface configureren \(BVI\)](#)
3. [Configureer de SSID's voor WAP-PSK-verificatie](#)
4. [Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

[Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)

Voltooi deze acties:

1. **Schakel IRB in de router in.**`router<configuratie>#bridge irb`**Opmerking:** Als alle security typen op één router ingesteld moeten worden, is deze voldoende om IRB slechts eenmaal mondiaal op de router mogelijk te maken. Het hoeft niet voor elk afzonderlijk authenticatietype te worden ingeschakeld.
2. **Definieer een bruggroep.**Dit voorbeeld gebruikt het bridge-group nummer `3`.`router<configuratie>#bridge 3`
3. **Kies het overspannen van een boomprotocol voor de bridge groep.**Het IEEE die in een boom protocol omspant wordt voor deze bridge groep geconfigureerd.`router<configuratie>#bridge 3 protocol-ieee`
4. **Laat een BVI toe om routeerbare pakketten die van zijn correspondent bridge groep worden ontvangen en te leiden.**Dit voorbeeld stelt de BVI in staat IP-pakketten te aanvaarden en te verzenden.`router<configuratie>#bridge 3 route-ip`

[De overbrugde virtuele interface configureren \(BVI\)](#)

Voltooi deze acties:

1. **Configureer de BVI.**Configureer de BVI wanneer u het corresponderende nummer van de bruggroep aan de BVI toewijst. Elke overbruggingsgroep kan slechts één correspondent BVI hebben. Dit voorbeeld kent bridge group nummer 3 toe aan de BVI.`router<configuratie>#interface BVI <2>`
2. **Geef een IP-adres aan de BVI toe.**`router<span-if>#ip-adres 10.1.1.1 255.255.0.0``router<span-if>#no afgesloten`

[Configureer de SSID's voor WAP-PSK-verificatie](#)

Voltooi deze acties:

1. **Schakel de radio-interface in.** Ga naar de configuratie-modus van de DOT11-radio om de interface te activeren en wijs een SSID aan de interface toe.
router#interface-punt11radio0router<span-if>#no shutdownrouter<Config-if>#ssid *wpa-gedeeld*
2. **Stel eerst het WAP-encryptie-algoritme voor de VLAN-interface in om het beheer van de WAP-toets in te schakelen.** Dit voorbeeld gebruikt tkip als encryptie algoritme.. Typ deze opdracht om het WAP-beheertype op de radio-interface te specificeren.
router#interface-punt11radio0router (configuratie-als)#encryptie VLAN 3 mode ciphers *tkip*
3. **Bind SSID aan een VLAN.** Om SSID op deze interface in te schakelen, bindt SSID aan het VLAN in de configuratie van SSID.
router<span-ssid>VLAN 3
4. **Configureer de SSID met de WAP-PSK-verificatie.** U dient eerst open of netwerk MAP verificatie in de SSID configuratie modus te configureren om het beheer van de WAP-toets mogelijk te maken. Dit voorbeeld vormt open authenticatie.
router#interface-punt11radio0router<Config-if>#ssid *wpa-gedeeld*router<span-ssid>#authenticatie openSchakel nu de WAP-toets in op de SSID. Het toetsenbord is al ingesteld voor dit VLAN.
router (configuratie-als-ssid)#authenticatie key-management wpaConfigureer de WAP-PSK-verificatie op de SSID.
router (configuratie-als-ssid)#wpa-psk ascii *1234567890!—1234567890 is de pre-gedeelde sleutelwaarde voor deze SSID. Zorg ervoor dat dezelfde toets voor deze SSID aan de clientzijde is gespecificeerd.*
5. **Schakel VLAN in op de radio-interface.**
router#interface Dot11Radio 0.3router<span-subif>#encapsulation dot1Q 3router<span-subif>#bridge-group 3

[Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

Typ deze opdrachten in de configuratie-modus wereldwijd om de interne DHCP-server voor de draadloze clients van dit VLAN te configureren:

- ip dhcp exclusief adres 10.3.1.1 10.3.1.5
- ip dhcp pool *wpa-psk*

Typ in de DHCP-podconfiguratie deze opdrachten:

- netwerk 10.3.0.0 255.255.0.0
- standaard-router 10.3.1.1

[WAP-verificatie configureren \(met EAP-verificatie\)](#)

Dit is een ander type van de sleutel van WAP beheer. Clients en de authenticatieserver authenticeren elkaar op basis van een MAP-verificatiemethode en de client en server genereren een paarsgewijze master key (PMK). Met WAP genereert de server de PMK dynamisch en geeft het door naar het toegangspunt, maar met WAP-PSK, vormt u een vooraf gedeelde toets op zowel de client als het access point, en die vooraf gedeelde toets wordt gebruikt als PMK.

Raadpleeg [WAP met EAP-verificatie](#) voor meer informatie.

Dit voorbeeld gebruikt deze configuratie instellingen:

- SSID-naam: **dot1x**
- VLAN 4
- Interne DHCP-serverbereik: **10.4.0.0/16**

Voltooi deze acties op de router:

1. [Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)
2. [De overbrugde virtuele interface configureren \(BVI\)](#)
3. [Configuratie van de Lokale RADIUS-server voor WAP-verificatie.](#)
4. [SSID voor WAP configureren met EAP-verificatie](#)
5. [Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

[Het geïntegreerde routing en bridging \(IRB\) configureren en de Bridge Group instellen](#)

Voltooi deze acties:

1. **Schakel IRB in de router in.**`router<configuratie>#bridge irb`**Opmerking:** Als alle security typen op één router ingesteld moeten worden, is deze voldoende om IRB slechts eenmaal mondiaal op de router mogelijk te maken. Het hoeft niet voor elk afzonderlijk authenticatietype te worden ingeschakeld.
2. **Definieert een Bridge Group.**Dit voorbeeld gebruikt bridge-group nummer **4**.`router<configuratie>#bridge 4`
3. **Selecteer het overspannen van een boomprotocol voor de bridge groep.**Hier wordt het IEEE die in een boom protocol omspant voor deze bridge groep geconfigureerd.`router<configuratie>#bridge 4-protocolreeks`
4. **Laat een BVI toe om de routeerbare pakketten die van zijn correspondent bridge groep worden ontvangen te aanvaarden en te leiden.**Dit voorbeeld stelt de BVI in staat IP-pakketten te aanvaarden en te verzenden.`router<configuratie>#bridge 4-route-ip`

[De overbrugde virtuele interface configureren \(BVI\)](#)

Voltooi deze acties:

1. **Configureer de BVI.**Configureer de BVI wanneer u het corresponderende nummer van de bruggroep aan de BVI toewijst. Elke overbruggingsgroep kan slechts één overeenkomend BVI hebben. Dit voorbeeld kent bridge group nummer 4 toe aan de BVI.`router<configuratie>#interface BVI <4>`
2. **Geef een IP-adres aan de BVI toe.**`router<span-if>#ip-adres 10.4.1.1 255.255.0.0``router<span-if>#no afgesloten`

[De lokale RADIUS-server voor WAP-verificatie configureren](#)

Raadpleeg het gedeelte onder [802.1x/EAP-verificatie](#) voor de gedetailleerde procedure.

[SSID voor WAP configureren met EAP-verificatie](#)

Voltooi deze acties:

1. **Schakel de radio-interface in.** Ga naar de configuratie-modus van de DOT11-radiointerface om de radio-interface te activeren en wijs een SSID aan de interface toe.

```
router<span>#interface-punt11radio0router<span-if>#no shutdownrouter<Config-if>#ssid wpa-dot1x
```
2. **Stel eerst het WAP-encryptie-algoritme voor de VLAN-interface in om het beheer van de WAP-toets in te schakelen.** Dit voorbeeld gebruikt *tkip* als encryptie algoritme.. Typ deze opdracht om het WAP-beheertype op de radio-interface te specificeren.

```
router<span>#interface-punt11radio0router (configuratie-als)#encryptie VLAN 4 mode ciphers tkip
```
3. **Bind SSID aan een VLAN.** Als u SSID op deze interface wilt activeren, bindt u de SSID aan het VLAN in de SSID-configuratiemodus.
VLAN 4
4. **Configureer de SSID met de WAP-PSK verificatie.** Om de radio-interface voor WAP te configureren met MAP-verificatie, moet u eerst de bijbehorende SSID voor netwerk EAP configureren.

```
router<span>#interface-punt11radio0router<Config-if>#ssid wpa-gedeeldrouter<span-ssid>#Authenticatie netwerk eap _methods
```
5. **Schakel nu de WAP-toets in op de SSID.** Het toetsenbord is al ingesteld voor dit VLAN.

```
router (configuratie-als-ssid)#authenticatie key-management wpa
```
6. **Schakel VLAN in op de radio-interface.**

```
router<span>#interface Dot11Radio 0.4router<span-subif>#encapsulation dot1Q 4router<span-subif>#bridge-group 4
```

[Het configureren van de interne DHCP-server voor de draadloze clients van dit VLAN](#)

Typ deze opdrachten in de configuratie-modus wereldwijd om de interne DHCP-server voor de draadloze clients van dit VLAN te configureren:

- ip dhcp exclusief adres 10.4.1.1 10.4.1.5
- ip dhcp pool *wpa-dot1gedeelde*

Typ in de DHCP-podconfiguratie deze opdrachten:

- netwerk 10.4.0.0 255.255.0.0
- Standaard-router 10.4.1.1

[Draadloze client voor verificatie configureren](#)

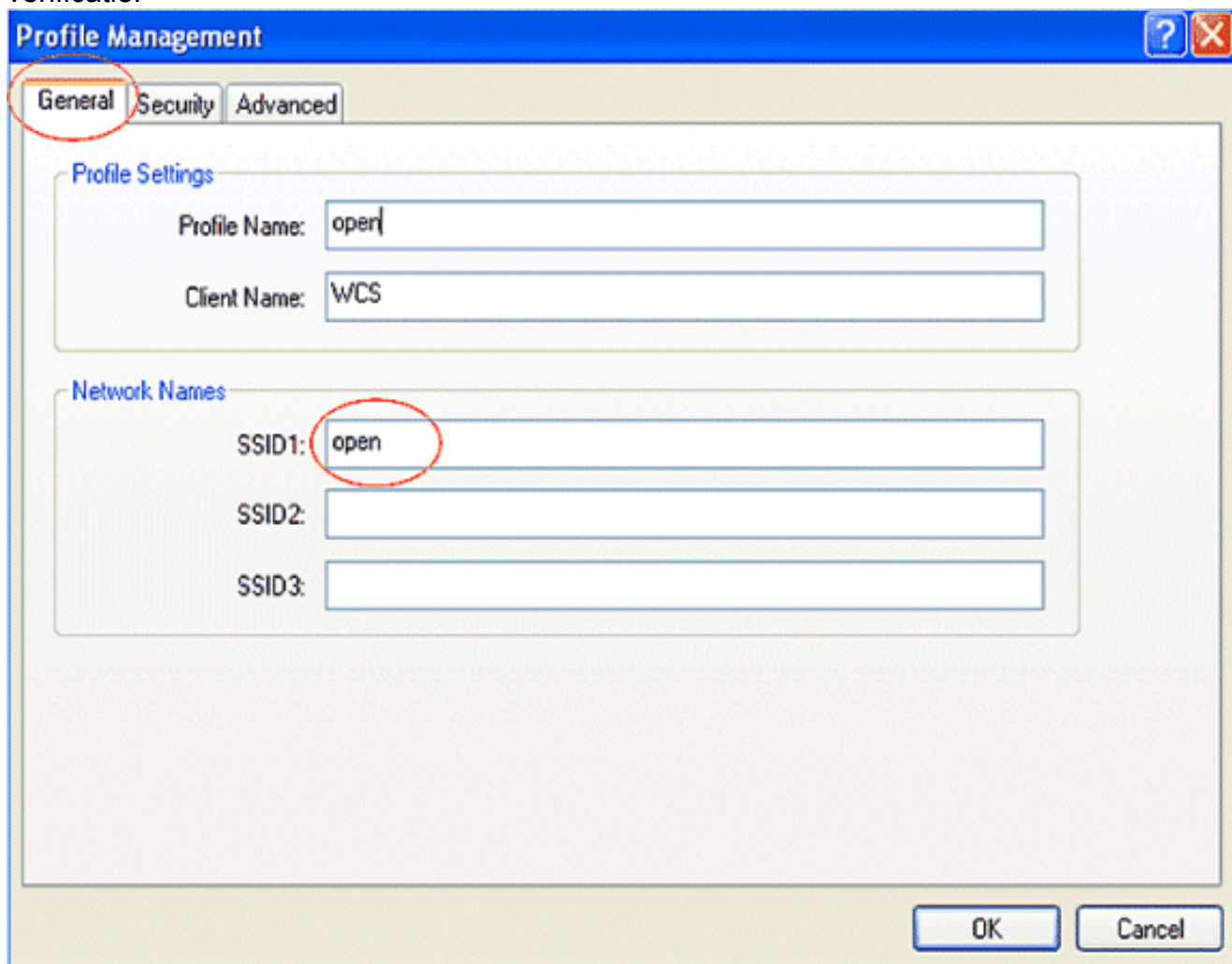
Nadat u ISR vormt, moet u de draadloze client voor verschillende authenticatietypen configureren zoals uitgelegd, zodat de router deze draadloze clients kan authenticeren en toegang tot het WLAN-netwerk kan bieden. Dit document maakt gebruik van Cisco Aironet Desktop Utility (ADU) voor de configuratie van de clientzijde.

[De draadloze client voor Open Verificatie configureren](#)

Voer de volgende stappen uit:

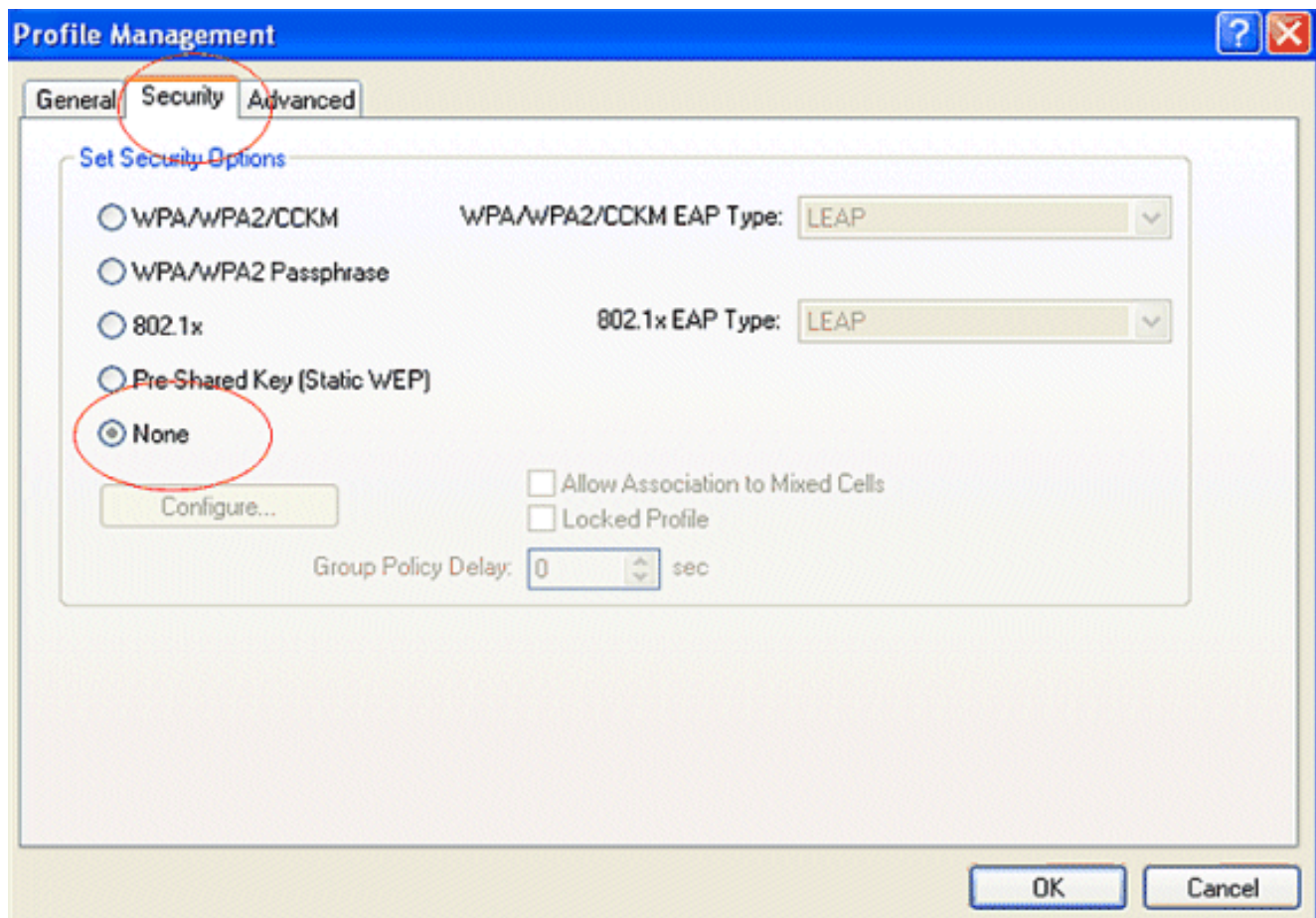
1. Klik in het venster Profile Management op de ADU op **New** om een nieuw profiel te maken. Een nieuw venster toont waar u de configuratie voor open authenticatie kunt instellen. Voer onder het tabblad **Algemeen** de naam van het profiel en de SSID in die de clientadapter gebruikt. In dit voorbeeld zijn de profielnaam en SSID **open**. **Opmerking:** SSID moet

overeenkomen met de SSID die u op ISR hebt ingesteld voor open verificatie.

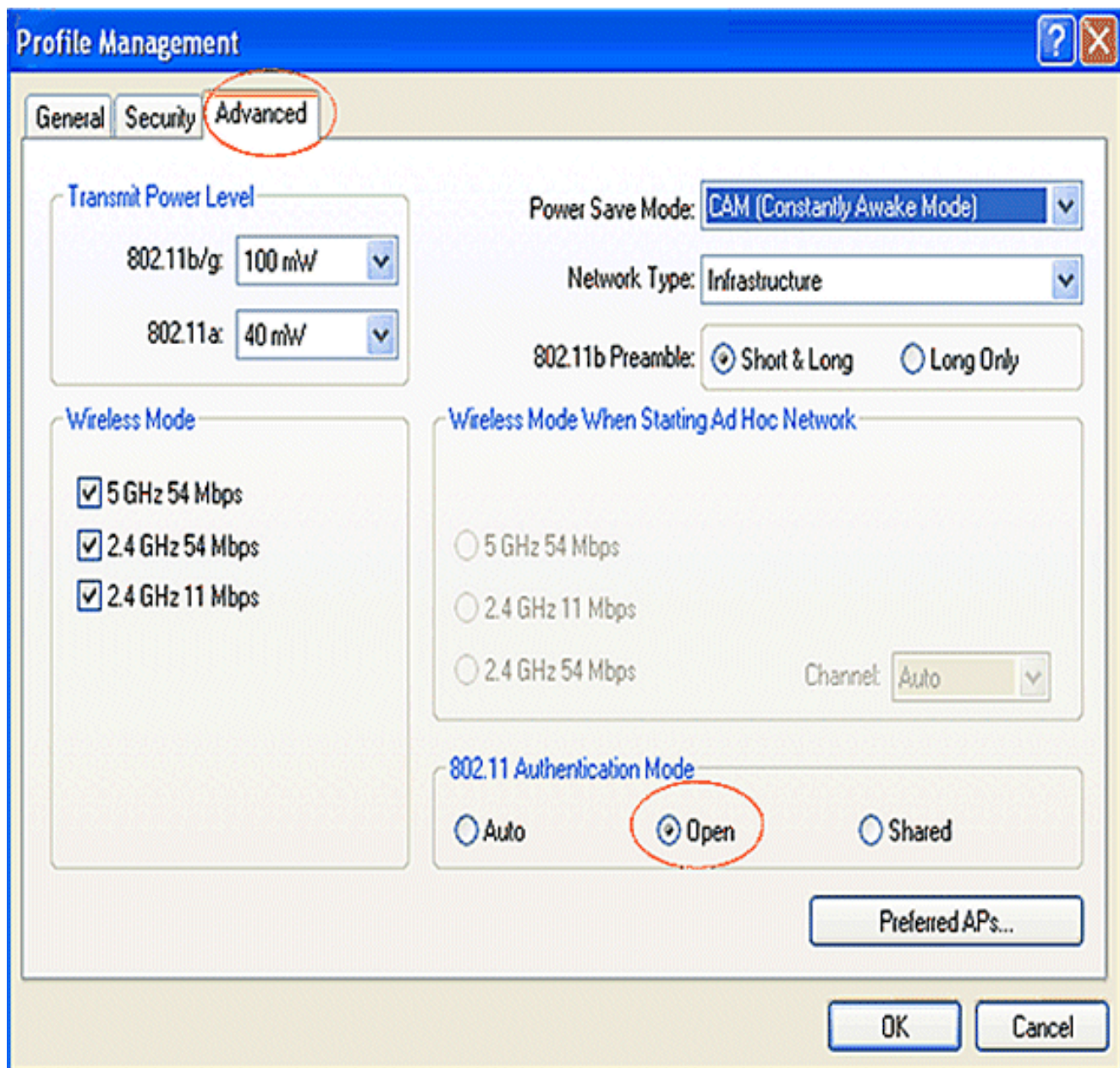


The image shows a 'Profile Management' dialog box with three tabs: 'General', 'Security', and 'Advanced'. The 'General' tab is selected and circled in red. Under 'Profile Settings', the 'Profile Name' field contains 'open' and the 'Client Name' field contains 'WCS'. Under 'Network Names', the 'SSID1' field contains 'open' and is circled in red. The 'SSID2' and 'SSID3' fields are empty. At the bottom right, there are 'OK' and 'Cancel' buttons.

2. Klik op het tabblad **Beveiliging** en laat de beveiligingsoptie als **Geen** voor de EFN-codering achter. Aangezien dit voorbeeld gebruikmaakt van EFN als optioneel, zal het instellen van deze optie op geen de client in staat stellen om met succes te associëren en te communiceren met het WLAN-netwerk. Klik op **OK**

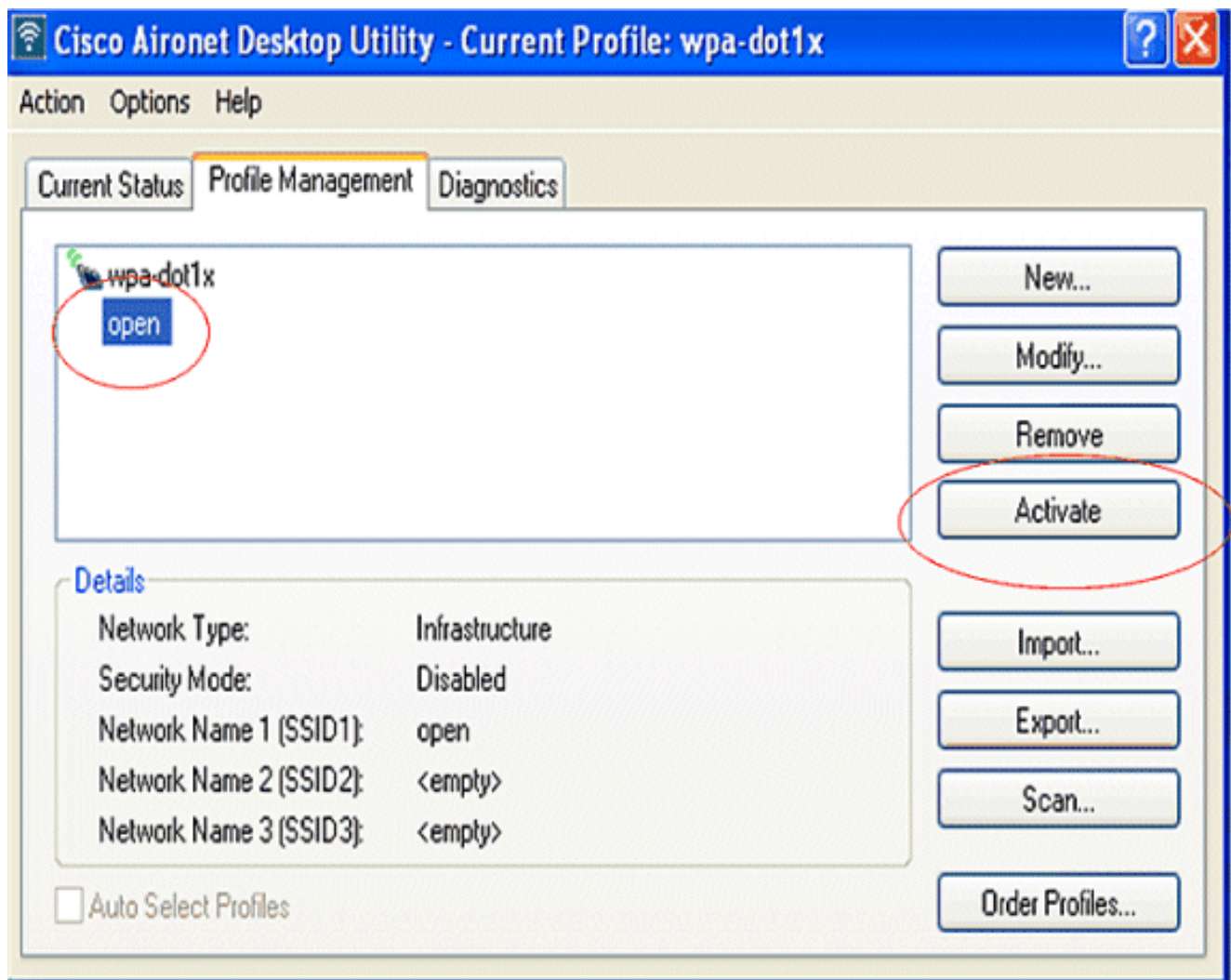


3. Selecteer het venster **Advanced** in het tabblad **Profile Management** en stel de 802.11-verificatiemodus in als **open** voor open verificatie.

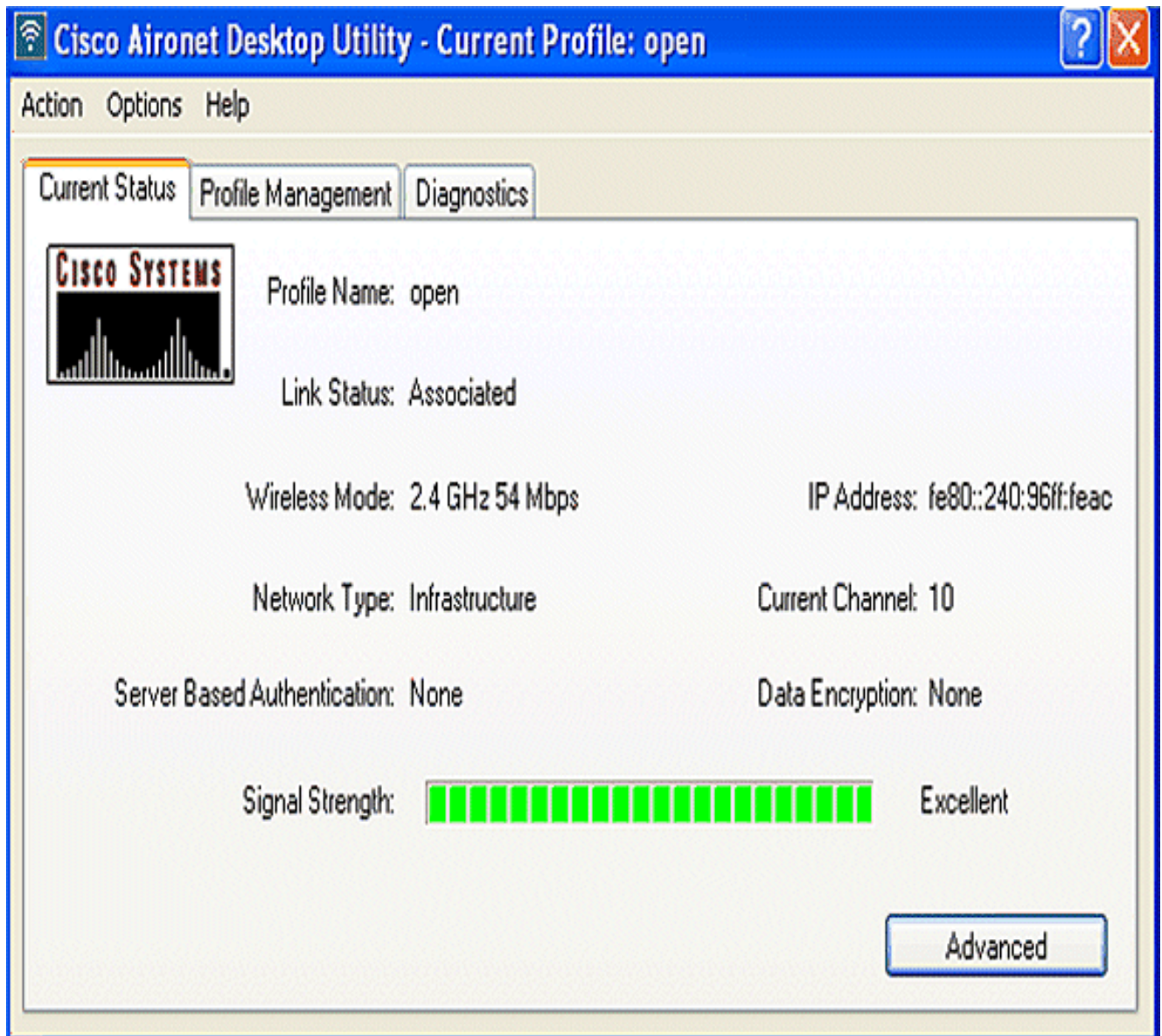


Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

1. Klik nadat het clientprofiel is gemaakt op **Activeren** onder het tabblad Profile Management om het profiel te activeren.



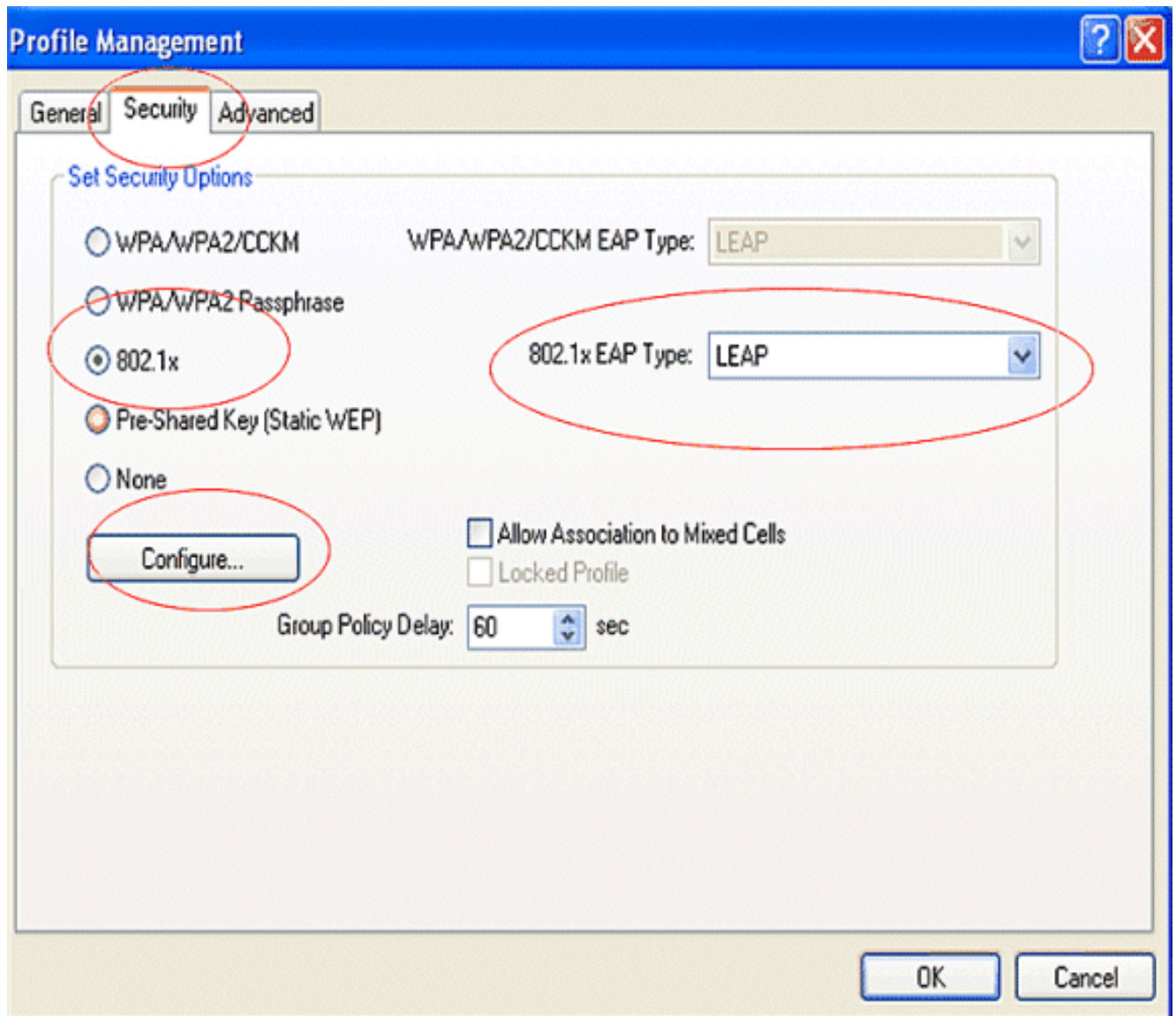
2. Controleer de ADU status voor een succesvolle verificatie.



[De draadloze client configureren voor 802.1x/EAP-verificatie](#)

Voer de volgende stappen uit:

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 open authenticatie kunt instellen. Voer onder het tabblad **Algemeen** de naam van het profiel en de SSID in die de clientadapter gebruikt. In dit voorbeeld, zijn de profielnaam en SSID **misleidend**.
2. Klik onder **Profile Management** op het **Security** tabblad, stel de beveiligingsoptie in als 802.1x en kies het juiste EAP-type. In dit document wordt LEAP gebruikt als het MAP-type voor authenticatie. Klik nu op **Configureren** om LEAP-instellingen voor gebruikersnaam en wachtwoord te configureren. **Opmerking:** Opmerking: SSID moet overeenkomen met de SSID die u op ISR hebt ingesteld voor 802.1x/EAP-verificatie.



3. Onder gebruikersnaam en wachtwoordinstellingen kiest dit voorbeeld ervoor om **handmatig de naam en het wachtwoord van de gebruiker te vragen**, zodat de client wordt gevraagd de juiste naam en het juiste wachtwoord in te voeren terwijl de client probeert verbinding te maken met het netwerk. Klik op **OK**.

LEAP Settings

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

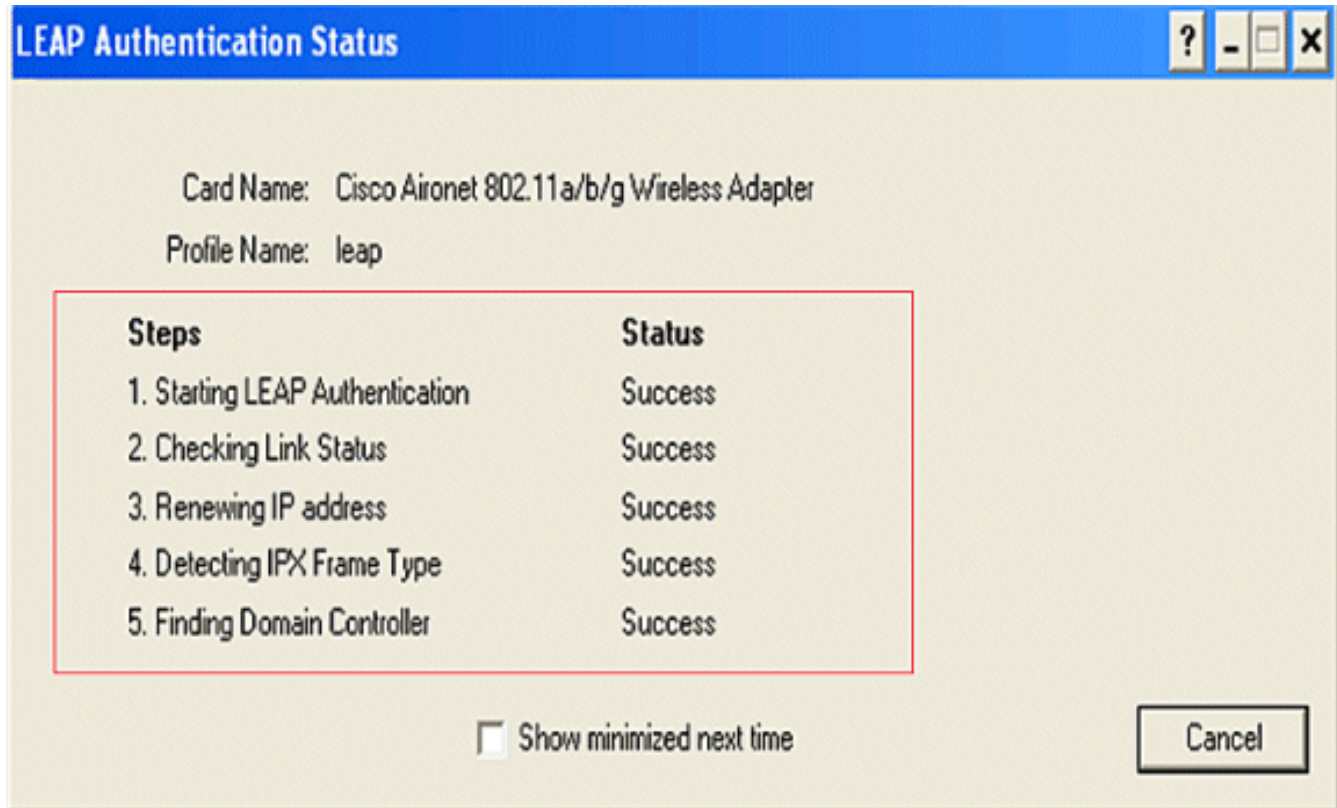
No Network Connection Unless User Is Logged In

Authentication Timeout Value (in seconds)

OK Cancel

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

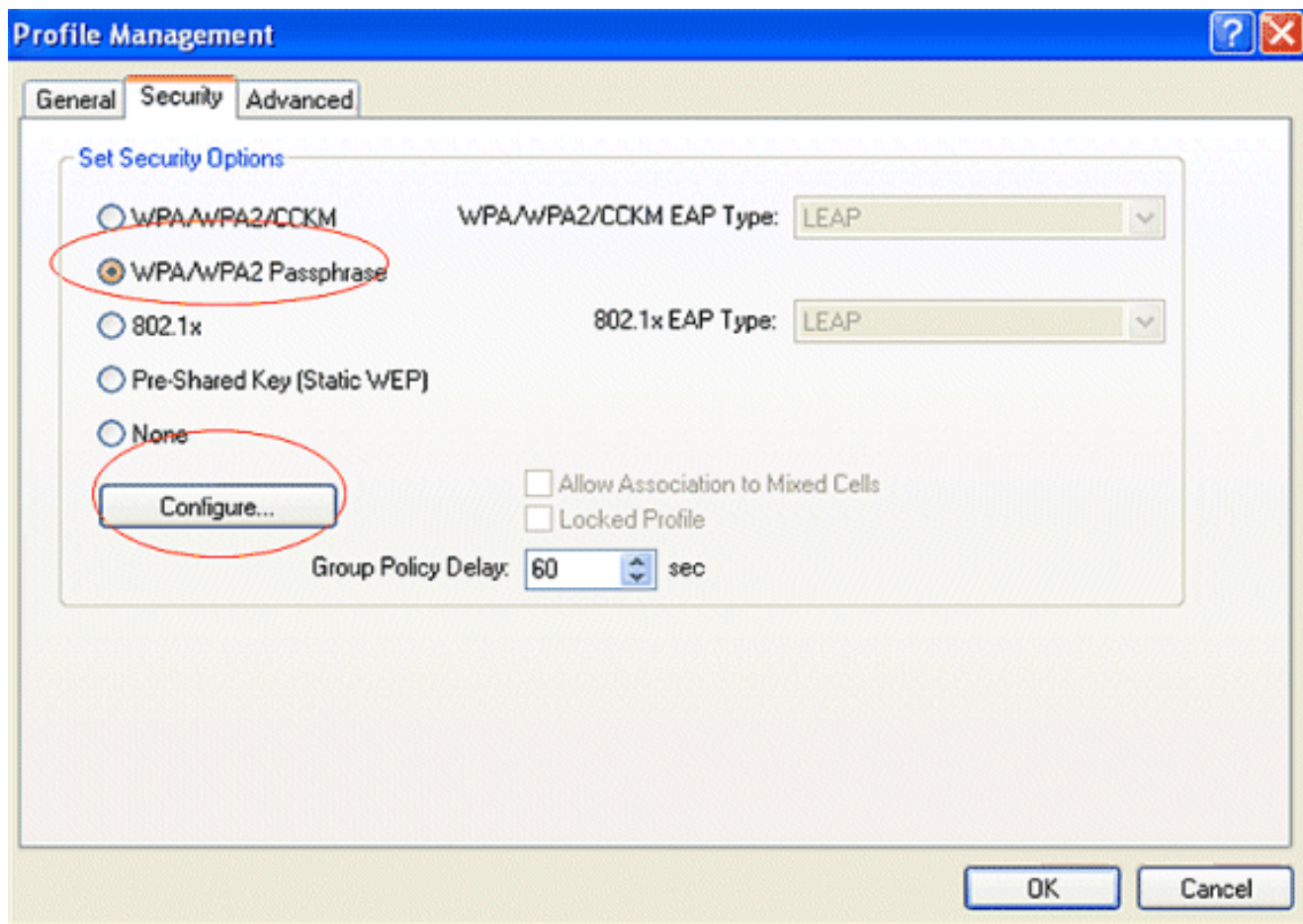
- Klik nadat het clientprofiel is gemaakt op **Activeren** onder het tabblad **Profielbeheer** om de **sprong** in het profiel te activeren. U wordt gevraagd de startnaam en het wachtwoord op te geven. Dit voorbeeld gebruikt de gebruikersnaam en het wachtwoord **gebruiker1**. Klik op **OK**.
- U kunt de client eerst controleren en vervolgens een IP-adres toegewezen krijgen van de DHCP-server die op de router is geconfigureerd.



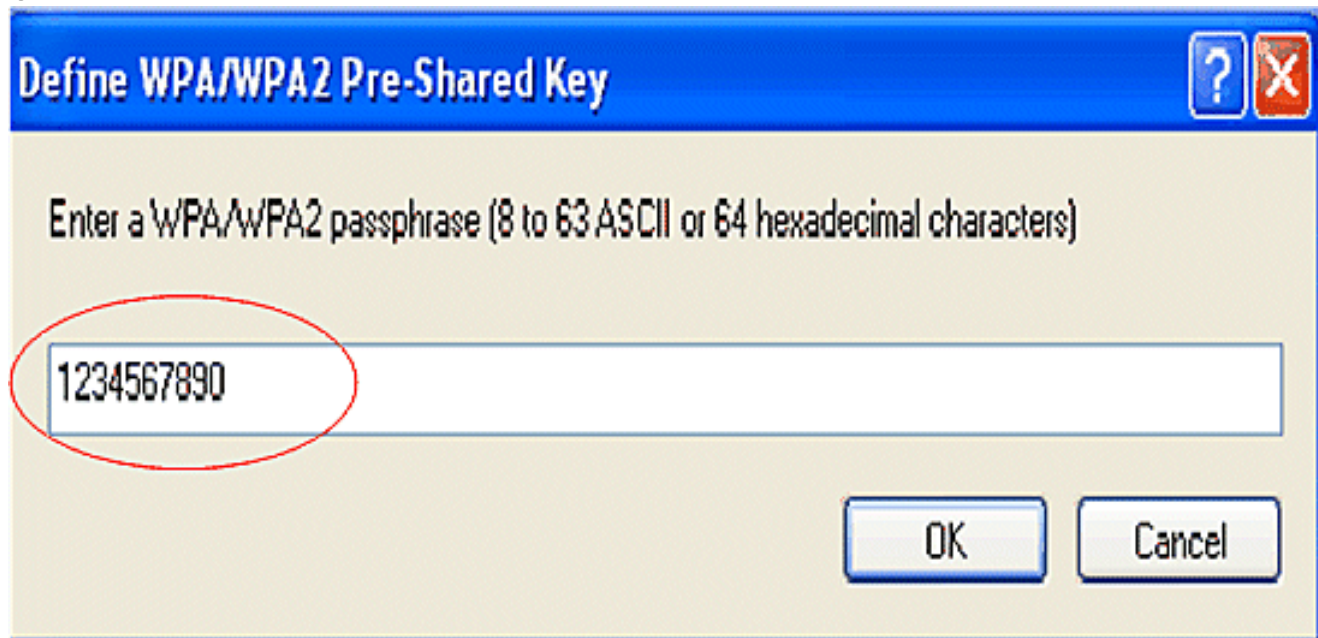
[De draadloze client voor WAP-PSK-verificatie configureren](#)

Voer de volgende stappen uit:

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 open authenticatie kunt instellen. Typ onder het tabblad **Algemeen** de **naam van het profiel** en **SSID** die de clientadapter gebruikt. In dit voorbeeld zijn de profielnaam en SSID **door de wpa gedeeld**. **OPMERKING:** SSID moet overeenkomen met de SSID die u op ISR voor de bevestiging van WAP-PSK hebt ingesteld.
2. Klik onder **Profielbeheer** op het **tabblad Beveiliging** en stel de beveiligingsoptie in als **WAP/WAP2-wachtwoord**. Klik nu op **Configureren** om het wachtwoord voor WAP te configureren.

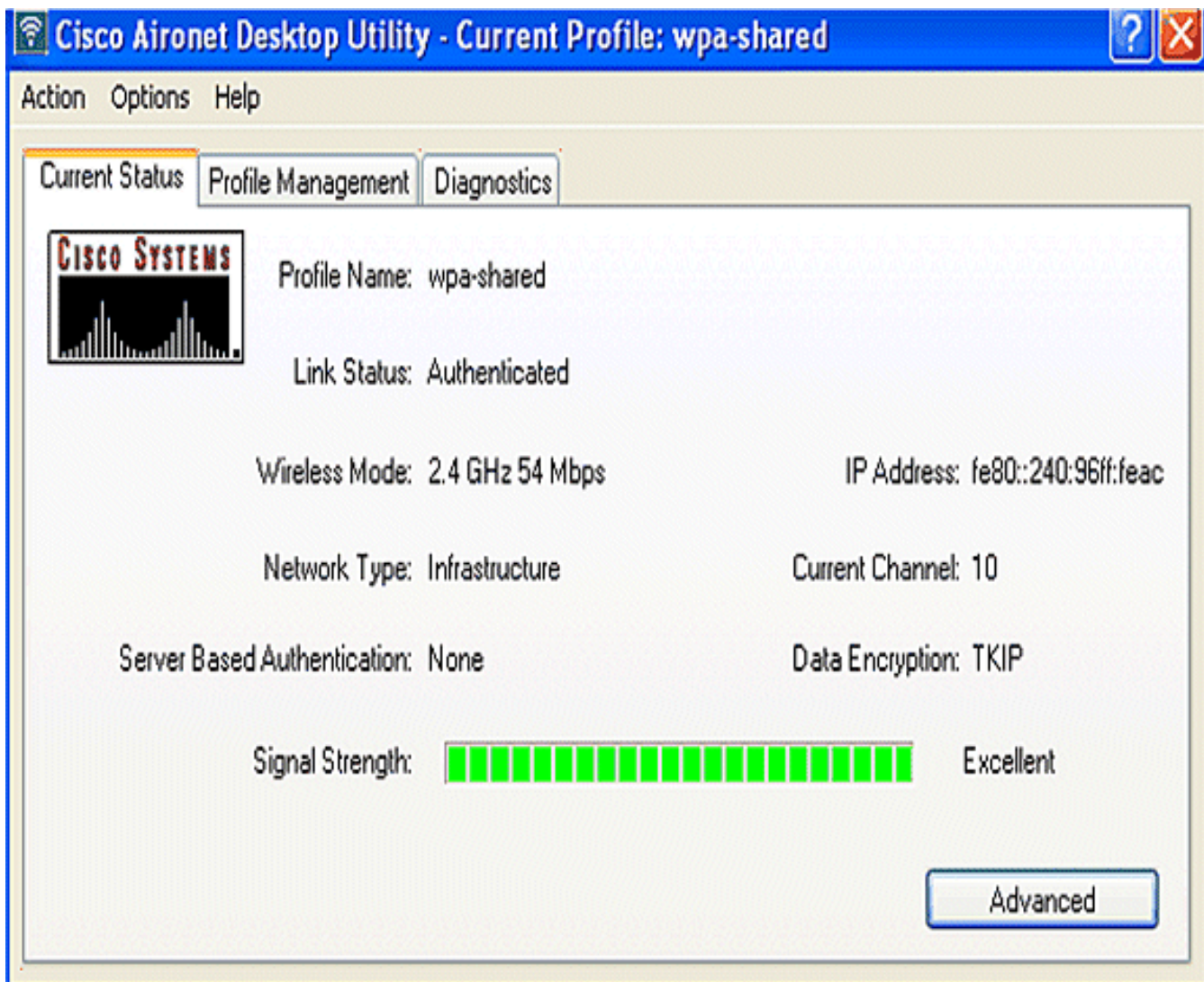


3. Definieer een voorgedeelde sleutel van WAP. De toets moet 8 tot 63 ASCII-teken lang zijn.
Klik op
OK.



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

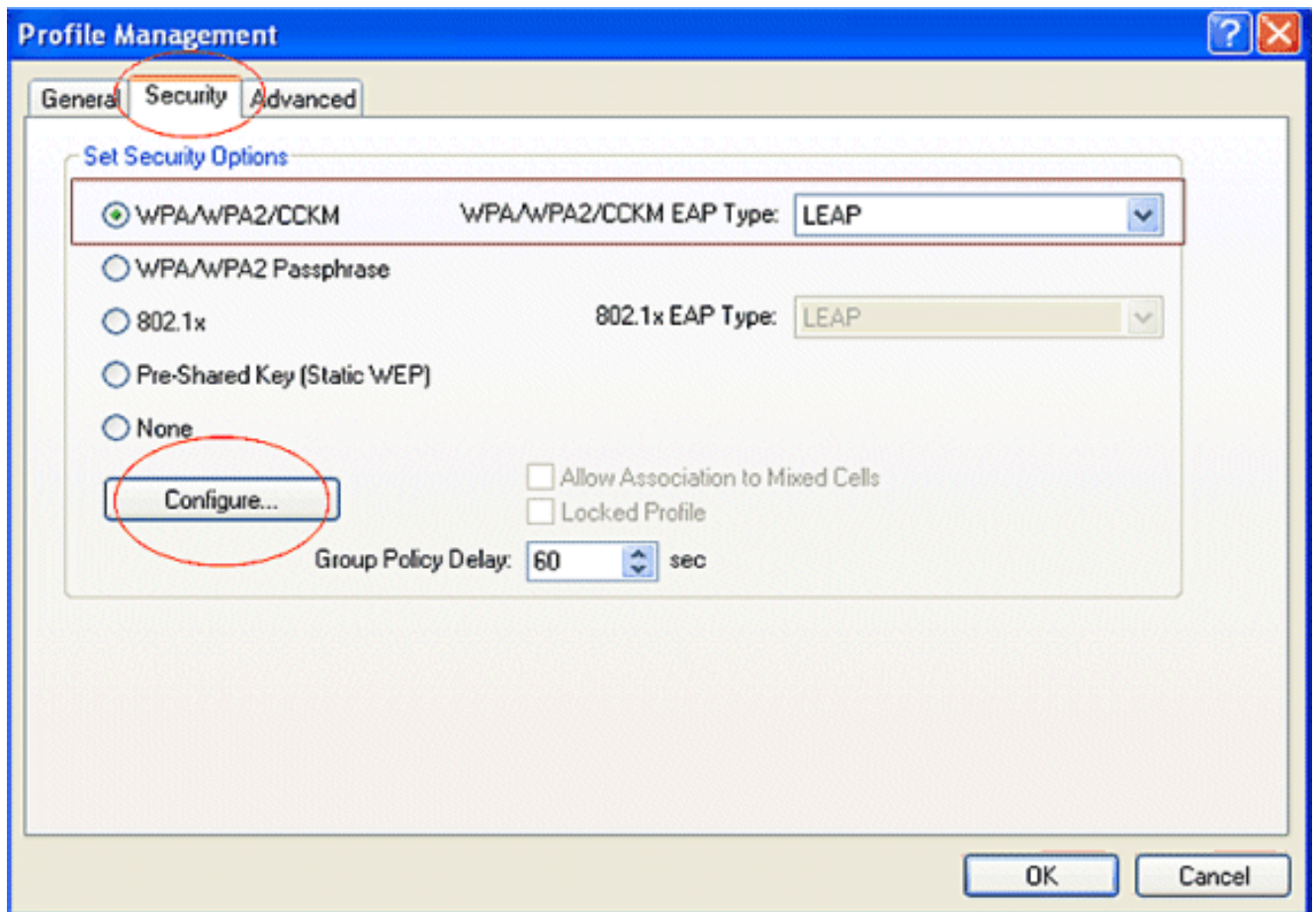
- Klik nadat het clientprofiel is gemaakt op **Activeren** onder het tabblad **Profielbeheer** om het **gedeelde profiel te activeren**.
- Controleer de ADU op een succesvolle authenticatie.



[De draadloze client voor WAP configureren \(met EAP\)](#)

Voer de volgende stappen uit:

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 open authenticatie kunt instellen. Voer onder het tabblad **Algemeen** de naam van het profiel in en SSID die de clientadapter gebruikt. In dit voorbeeld zijn de profielnaam en SSID **wpa-dot1x**. **Opmerking:** SSID moet overeenkomen met de SSID die u op ISR voor WAP (met EAP)-verificatie hebt ingesteld.
2. Klik onder **Profielbeheer** op het **tabblad Beveiliging**, stel de beveiligingsoptie in als **WAP/WAP2/CCKM** en kies het juiste type voor WAP/WAP2/CCKM EAP. In dit document wordt LEAP gebruikt als het MAP-type voor authenticatie. Klik nu op **Configureren** om LEAP-instellingen voor gebruikersnaam en wachtwoord te configureren.



3. Onder het gebied Gebruikersnaam en Wachtwoord Instellingen kiest dit voorbeeld **Handmatig voor Gebruikersnaam en Wachtwoord** zodat de client wordt gevraagd de juiste naam en het juiste wachtwoord in te voeren terwijl de client probeert verbinding te maken met het netwerk. Klik op **OK**.

LEAP Settings

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)

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

1. Klik nadat het clientprofiel is gemaakt op **Activeren** onder het tabblad Profile Management om het profiel **wpa-dot1x** te activeren. U wordt gevraagd om de naam en het wachtwoord van de MAP-gebruiker. Dit voorbeeld gebruikt gebruikersnaam en wachtwoord als **gebruiker1**.
Klik op
OK.

Enter Wireless Network Password

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

User Name :

Password :

Log on to :

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

Profile Name : wpa-dot1x

2. U kunt de client echt maken.

LEAP Authentication Status

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

Profile Name: wpa-dot1x

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

De opdracht **toont dot11-associaties** van de router CLI volledige details over de status van de

clientassociatie. Hierna volgt een voorbeeld.

Routerberichten#show dot11-associaties

802.11 Client Stations on Dot11Radio0:

SSID [leap] :

MAC Address	IP address	Device	Name	Parent	State
0040.96ac.e657	10.3.0.2	CB21AG/PI21AG	WCS	self	EAP-Assoc

SSID [open] :

SSID [pre-shared] : DISABLED, not associated with a configured VLAN

SSID [wpa-dot1x] :

SSID [wpa-shared] :

Others: (not related to any ssid)

Problemen oplossen

Opdrachten voor troubleshooting

U kunt deze debug opdrachten gebruiken om problemen met uw configuratie op te lossen.

- **debug dot11 a authenticator alle** - activeert het fouilleren van MAC en EAP authenticatiepakketten.
- **detectie straal**-displays de RADIUS-onderhandelingen tussen de server en client.
- **bug van lokale serverpakketten**-Hiermee geeft u de inhoud van de RADIUS-pakketten weer die worden verzonden en ontvangen.
- **bug van Straal client-server client**-Hier worden foutmeldingen over mislukte client-authenticaties weergegeven.

Gerelateerde informatie

- [Verificatie van configuratievoorbeelden voor draadloze LAN-controllers](#)
- [VLAN's configureren op access points](#)
- [1800 ISR draadloze router met interne DHCP en open verificatie Configuratievoorbeeld](#)
- [Configuratie-handleiding voor Cisco draadloos ISR en HWIC access point](#)
- [Draadloze LAN-connectiviteit met behulp van een ISR met EFN-encryptie en LEAP-verificatievoorbeeld](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)
- [Verificatietypen configureren](#)
- [Draadloze LAN-connectiviteit met behulp van een ISR met EFN-encryptie en LEAP-verificatievoorbeeld](#)