

Configuratievoorbeeld van draadloze LAN-verbinding

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[Conventies](#)

[Configuratie](#)

[Het access point configureren](#)

[Stapsgewijze instructies](#)

[De draadloze clientadapter configureren](#)

[Stapsgewijze instructies](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document biedt een voorbeeldconfiguratie die toont hoe u een fundamentele draadloze LAN (WLAN) verbinding kunt instellen met het gebruik van een Cisco Aironet Access Point (AP) en computers met Cisco-compatibele clientadapters. Het voorbeeld gebruikt de GUI.

Voorwaarden

Vereisten

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

Bekendheid met RF-technologie (basisradiofrequentie)

Basis begrip van hoe u toegang hebt tot een Cisco AP

Dit document gaat ervan uit dat de stuurprogramma's van de draadloze clientkaarten voor de pc's of laptops al geïnstalleerd zijn.

Gebruikte componenten

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

Eén Aironet 1200 Series AP die Cisco IOS® software release 12.3(7)JA runt

Drie Aironet 802.11a/b/g clientadapters die firmware 2.5 uitvoeren

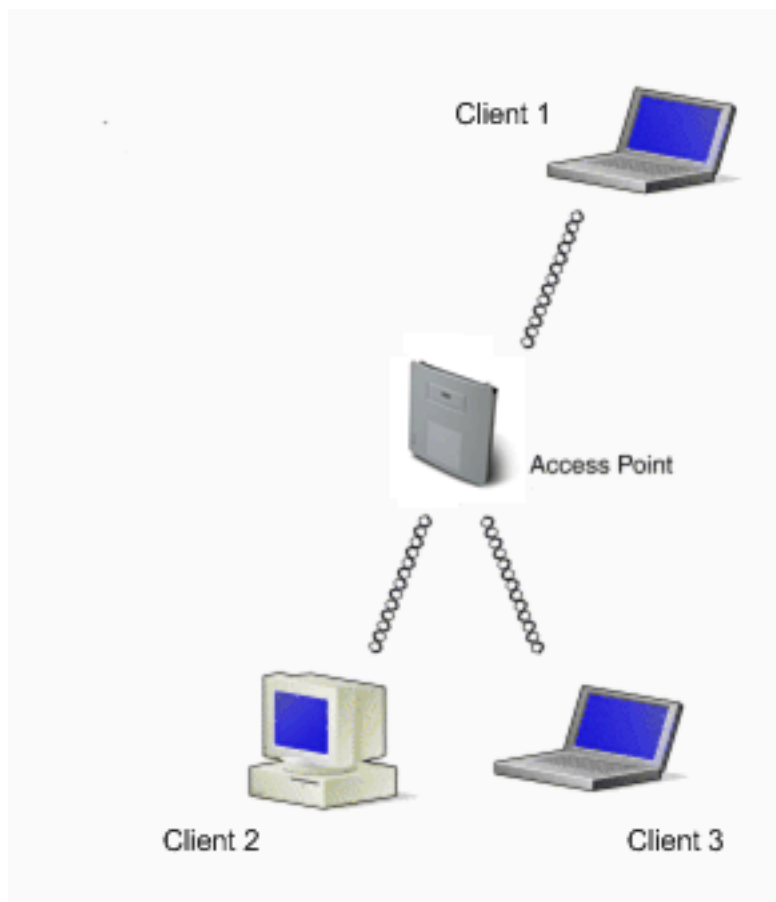
Aironet Desktop Utility (ADU) versie 2.5

Opmerking: dit document gebruikt een AP met een geïntegreerde antenne. Als u AP gebruikt dat een externe antenne vereist, zorg er dan voor dat de antennes op AP worden aangesloten. Anders kan AP niet met het draadloze netwerk verbinden. Bepaalde AP-modellen hebben geïntegreerde antennes, terwijl andere een externe antenne nodig hebben voor algemene werking. Raadpleeg voor informatie over de AP-modellen met interne of externe antennes 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 actief is, zorg er dan voor dat u de mogelijke impact van een opdracht of instelling in de GUI begrijpt.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Het netwerkdigram is drie Aironet 802.11a/b/g clientadapters die zijn aangesloten op een 1200 AP. Dit document beschrijft de configuratie van de clientadapters om met elkaar te communiceren via draadloze interface via de AP.

AP gebruikt deze instellingen:

Identificatiecode van de serviceset (SSID): **CISCO123-SYSTEEM**

Basisauthenticatie: Open verificatie met Wired Equivalent Privacy (EFN)-encryptie

In dit document worden de configuratie op de AP en de clientadapters uitgelegd.

Opmerking: U kunt ook andere authenticatie- en encryptiemethoden gebruiken. Zie [Verificatietypen configureren](#) voor informatie over de verschillende ondersteunde verificatiemechanismen. Raadpleeg voor informatie over de verschillende coderingsmechanismen die worden ondersteund de [Cipr-formaten](#) en de [finale](#)-coderingsmechanismen.

Conventies

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

Configuratie

Het access point configureren

U kunt AP met het gebruik van om het even welke van deze configureren:

GUI

Opdracht-line interface (CLI), nadat u een Telnet-sessie hebt ingesteld

De console poort

Opmerking: Om verbinding te maken met AP door de console poort, sluit u een negen-pins, rechte-door-DB-9 seriekabel aan op de RS-232 seriële poort op het AP en op de COM poort op een computer. Stel een terminalemulator in om met de AP te communiceren. Gebruik deze instellingen voor de aansluiting van de eindemulator:

9600 baud

8 gegevensbits

Geen pariteit

1 stopcontact

Geen stroomregeling

N.B.: Deze instellingen zijn de standaardinstellingen. Als u geen toegang tot het apparaat hebt nadat u het eindprogramma op de instellingen hebt ingesteld, kan het probleem zijn dat het apparaat niet op de standaardinstellingen is ingesteld. Probeer andere instellingen en start met de basissnelheid. Raadpleeg voor meer informatie over de specificaties van de console-kabel de [aansluiting op de 1200 en 1230AG Series access points](#) voor het [eerst in de buurt](#)

[van het configureren van het access point.](#)

In dit document wordt uitgelegd hoe u AP met het gebruik van de GUI kunt configureren.

Er zijn twee manieren om toegang te krijgen tot AP met het gebruik van de GUI:

Pas een IP-adres aan het apparaat toe voordat u een verbinding maakt met de GUI.

Verkrijg een IP adres met het gebruik van DHCP.

De verschillende modellen van Aironet APs vertonen verschillend standaard IP adresgedrag. Wanneer u een Aironet 350, 1130AG, 1200 of 1240AG Series AP met een standaardconfiguratie aan uw LAN-netwerk aansluit, vraagt AP een IP-adres van uw DHCP-server aan. Als het AP geen adres ontvangt, blijft het verzoeken voor onbepaalde tijd verzenden.

Wanneer u een Aironet 1100 Series AP met een standaardconfiguratie aan uw LAN aansluit, doet AP verschillende pogingen om een IP adres van de DHCP-server te krijgen. Als AP geen adres ontvangt, wijst het zichzelf het IP adres 10.0.0.1 voor 5 minuten toe. Tijdens deze periode van 5 minuten kunt u naar het standaard IP-adres bladeren en een statisch adres configureren. Als na de 5 minuten AP niet opnieuw wordt gevormd, gooit AP het 10.0.0.1 adres weg en vraagt een adres van de server van DHCP. Indien het AP geen adres ontvangt, stuurt het verzoeken voor onbepaalde tijd. Als u het venster van 5 minuten om op 10.0.1 naar de AP te bladeren, mist, kunt u het AP-programma inschakelen om het proces te herhalen.

Het netwerk in dit document gebruikt een AP van 1200 reeksen. Met een inlognaam via de console wordt AP gevormd met een statisch IP adres van 10.0.0.1. Raadpleeg voor informatie over de manier waarop IP-adressen aan AP worden toegewezen het [gedeelte IP-adres verkrijgen en toewijzen van het voor het eerst configureren van het access point](#).

[Stapsgewijze instructies](#)

Na het configureren van het IP-adres kunt u toegang krijgen tot AP via de browser om AP te configureren om client associatieverzoeken van client adapter te aanvaarden.

Voer de volgende stappen uit:

Voltooi de volgende stappen om toegang te krijgen tot AP met de GUI en het venster Summary Status te krijgen:

Open een webbrower en voer **10.0.0.1** in de adreslijn in.

Druk op **Tab** om het veld Gebruikersnaam te omzeilen en gaat naar het veld Wachtwoord.

Het venster Wachtwoord voor netwerk invoeren toont.

Voer het hoofdlettergevoelige wachtwoord in **Cisco** en druk op **ENTER**.

Het venster Summary Status toont, zoals dit voorbeeld toont:

Close Window

CISCO SYSTEMS

Cisco 1200 Access Point

Hostname AP1200 AP1200 uptime is 2 weeks, 6 days, 22 hours, 17 minutes

HOME

- EXPRESS SET-UP
- NETWORK MAP +
- ASSOCIATION
- NETWORK INTERFACES +
- SECURITY +
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

Home: Summary Status

Association

Clients: [0](#) Repeaters: [0](#)

Network Identity

IP Address: 10.0.0.1
 MAC Address: 000e.d7e4.a629

Network Interfaces

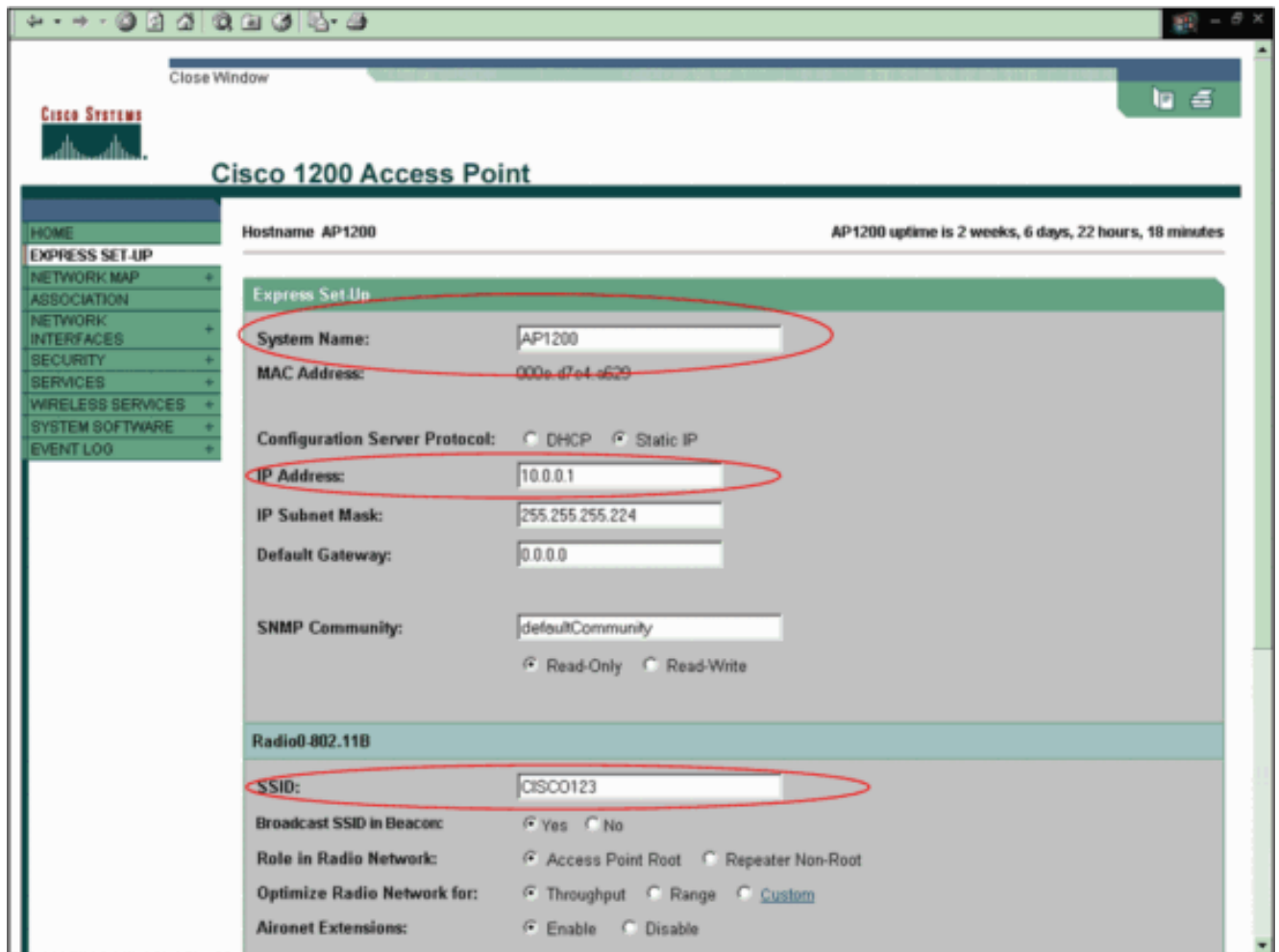
Interface	MAC Address	Transmission Rate
FastEthernet	000e.d7e4.a629	100Mb/s
Radio0-802.11B	000d.eded.7086	11.0Mb/s
Radio1-802.11A	000e.8405.0cb3	54.0Mb/s

Event Log

Time	Severity	Description
Mar 21 22:17:29.470	◆ Notification	Configured from console by cisco on vty0 (10.0.0.3)
Mar 21 22:17:27.922	◆ Error	Interface Dot11Radio0, changed state to up
Mar 21 22:17:27.902	◆ Notification	Interface Dot11Radio0, changed state to reset
Mar 21 22:17:27.902	◆ Error	Interface Dot11Radio1, changed state to up
Mar 21 22:17:27.896	◆ Notification	Interface Dot11Radio1, changed state to reset
Mar 21 22:15:31.691	◆ Notification	Line protocol on interface FastEthernet0, changed state to up

Klik op **Express Setup** in het menu links.

Het Express Setup-venster toont. U kunt dit venster gebruiken om een aantal van de fundamentele parameters te configureren die nodig zijn om een draadloze verbinding tot stand te brengen. Gebruik het venster Express Setup op AP 1200 om de acceptatie van draadloze clientassociaties te configureren. Hier is een voorbeeld van het venster:



Voer de configuratieparameters in de juiste velden in in het Express Setup-venster in.

De configuratieparameters omvatten deze parameters:

De naam van de gastheer van AP

IP-adresconfiguratie van het AP, als het adres een statische IP is

Standaard gateway

Simple Network Management Protocol (SNMP)-community-string

Rol in het radionetwerk

SSID

Dit voorbeeld stelt deze parameters in:

IP-adres: 10.0.0.1

Host name: **AP1200**

SSID: **CISCO123-SYSTEEM**

Opmerking: SSID's zijn unieke identificatoren die een WLAN-netwerk identificeren. Draadloze apparaten gebruiken SSID's om draadloze connectiviteit in te stellen en te onderhouden. SSID's zijn hoofdlettergevoelig en kunnen maximaal 32 alfanumerieke tekens bevatten. Gebruik geen spaties of speciale tekens in een SSID.

Opmerking: de overige parameters blijven standaard waarden gebruiken.

Klik op **Toepassen** om uw instellingen op te slaan.

Volg deze stappen om de radio-instellingen in te stellen:

Klik op **Netwerkinterfaces** in het menu links om naar de overzichtspagina van de netwerkinterfaces te bladeren.

Selecteer de radio-interface die u wilt gebruiken.

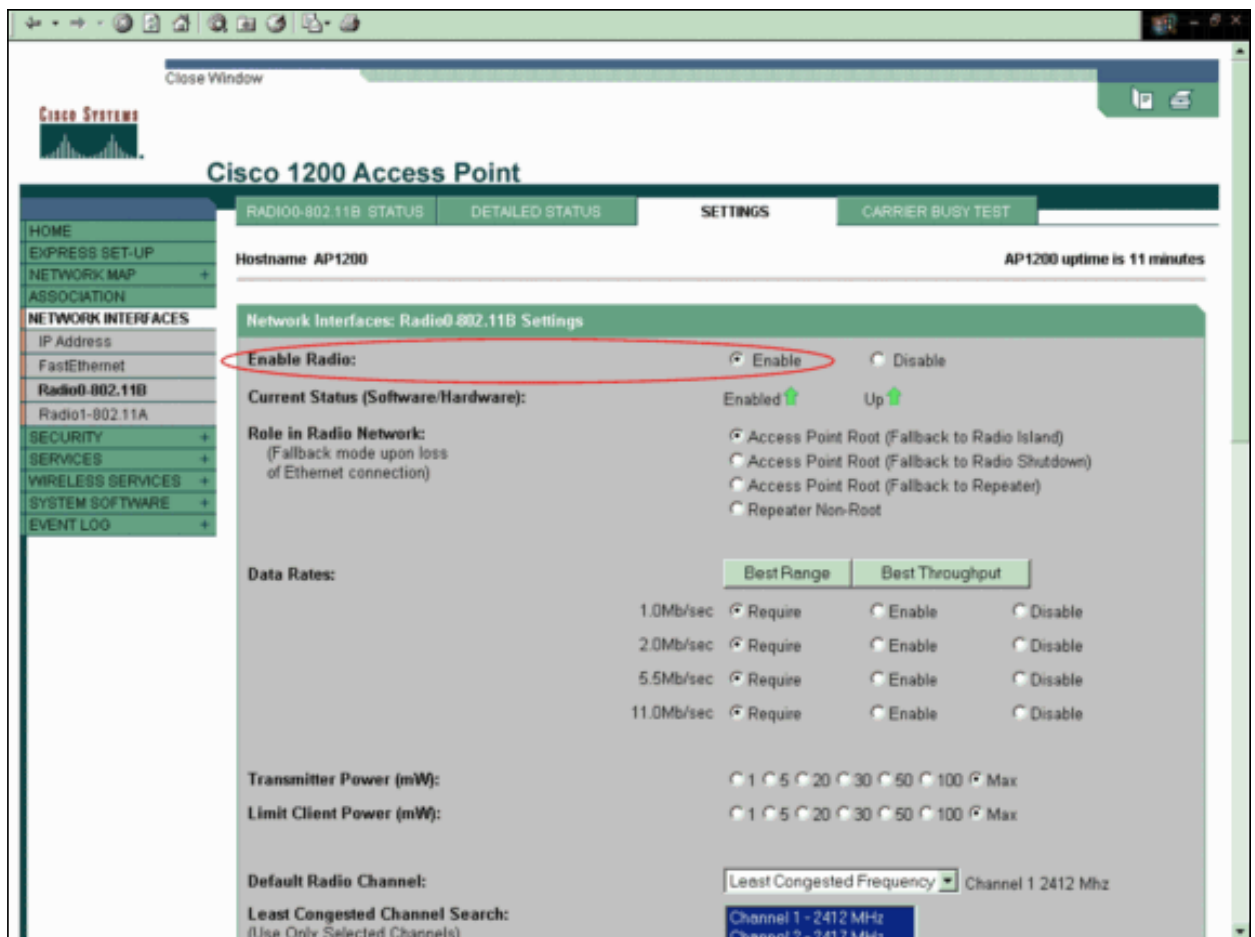
Dit voorbeeld gebruikt de interface Radio0-802.11B. Dankzij de actie kunt u naar de netwerkinterfaces bladeren: Radio Status pagina

Klik op het tabblad **Instellingen** om naar de pagina Instellingen voor de radio-interface te bladeren.

Klik op **Inschakelen** om de radio in te schakelen.

Laat alle andere instellingen op de pagina staan met de standaardwaarden.

Scrollt beneden en klik op **Toepassen** onder in de pagina om de instellingen op te slaan.



Voltooi de volgende stappen om SSID's en open authenticatie met behulp van EFG-encryptie te configureren:

Kies **Beveiliging > SSID Manager** in het menu links.

De pagina van SSID Manager toont.

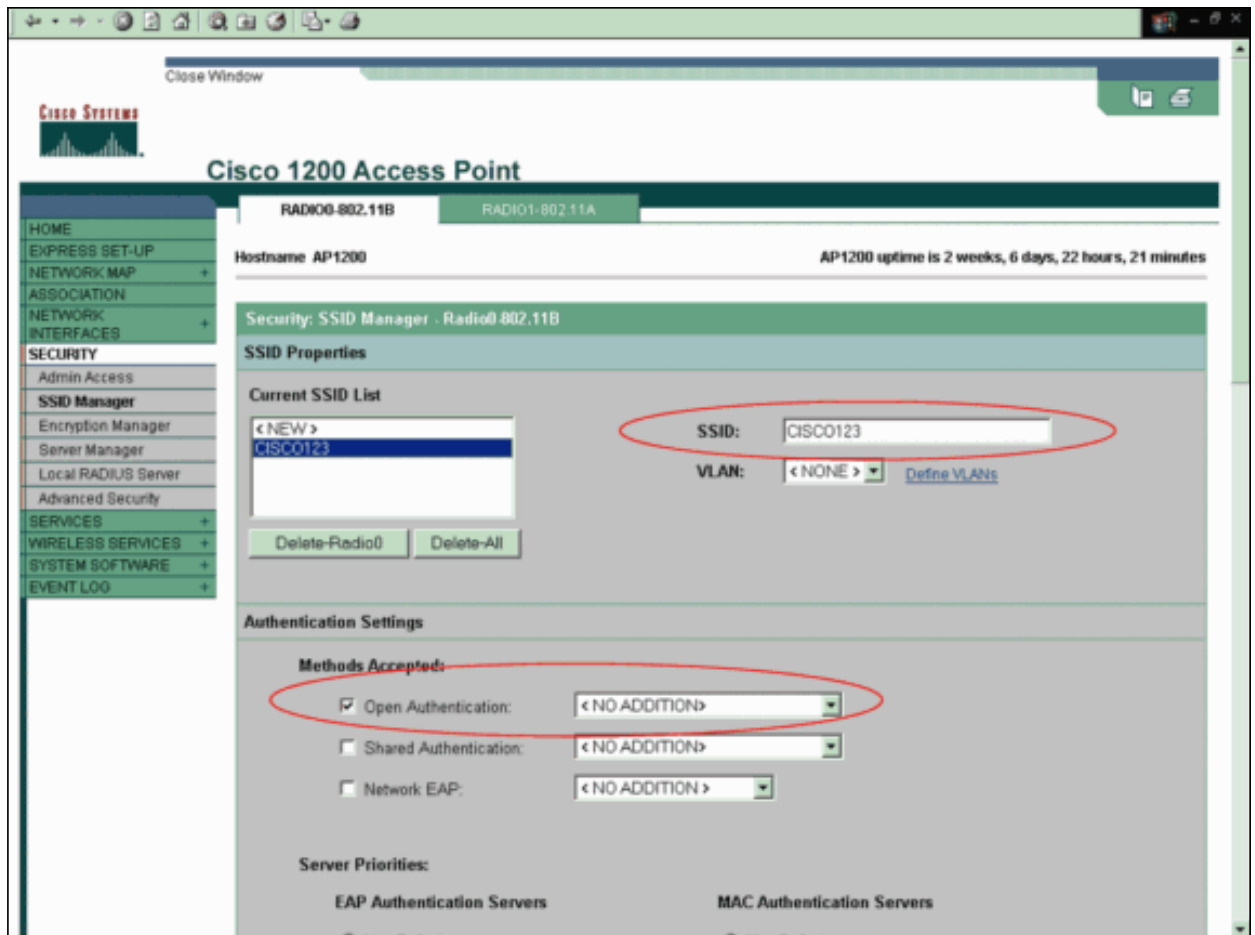
Selecteer SSID dat u in Stap 3 hebt gemaakt in het menu Huidige SSID-lijst.

Dit voorbeeld gebruikt CISCO123 als SSID.

Selecteer onder Verificatie Instellingen **Open Verificatie**.

Laat alle andere parameters met hun standaardwaarden zitten.

Klik op **Toepassen** onder in de pagina.



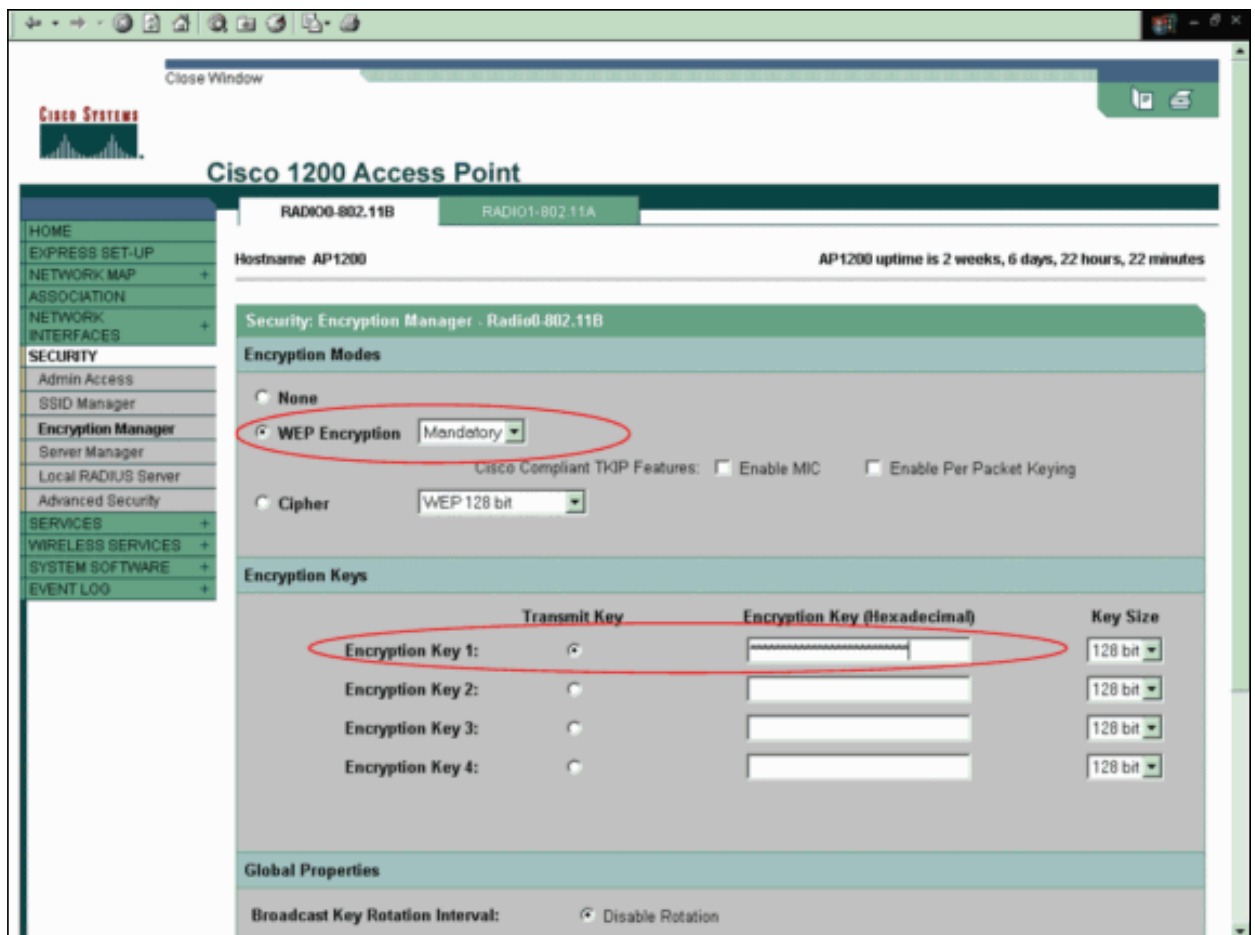
Voltooi de volgende stappen om de sleutels van EFN te configureren:

Kies **Security > Encryption Manager**.

Klik op **de Encryptie** van EFG onder de modi Encryption en kies de optie **Verplicht** in het vervolgkeuzemenu.

Voer de coderingssleutel van EFN in het gebied Encryption Keys in.

De de encryptiesleutels van EFN kunnen 40 bits of 128 bits in lengte zijn. Dit voorbeeld gebruikt de 128-bits coderingscode van **1234567890abcdef1234567890**.



Klik op **Toepassen** om de instellingen op te slaan.

[De draadloze clientadapter configureren](#)

Voordat u de clientadapter installeert, moet u de componenten van de clientadapteradapter en clientadaptersoftware op de pc of laptop installeren. Raadpleeg voor informatie over het installeren van de stuurprogramma's en hulpprogramma's voor de clientadapter [de clientadapter installeren](#).

[Stapsgewijze instructies](#)

Nadat u de clientadapter op de machine hebt geïnstalleerd, kunt u deze configureren. In deze paragraaf wordt uitgelegd hoe u de clientadapter moet configureren.

Voer de volgende stappen uit:

Maak een profiel op de ADU voor de clientadapter.

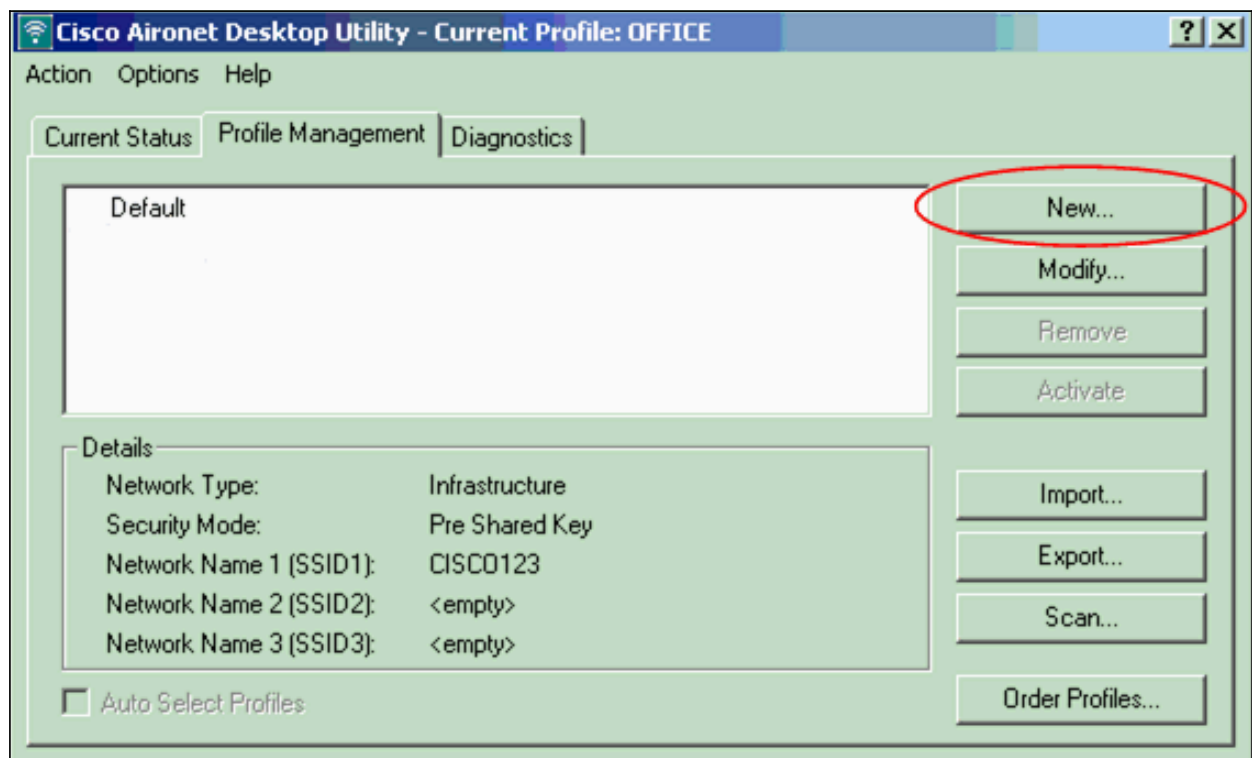
In het profiel worden de configuratie-instellingen gedefinieerd die de clientadapter gebruikt om verbinding te maken met het draadloze netwerk. U kunt maximaal 16 verschillende profielen op de ADU configureren. U kunt op basis van uw behoeften tussen de verschillende geconfigureerde profielen switches. Met profielen kunt u de clientadapter op verschillende locaties gebruiken, waarvoor verschillende configuratie-instellingen nodig zijn. Stel dat u profielen wilt instellen voor het gebruik van de clientadapter op kantoor, thuis en in openbare gebieden, zoals luchthavens of hotspots.

Voltooi de volgende stappen om een nieuw profiel te maken:

Klik op het tabblad **Profielbeheer** in de automatische documentinvoer.

Klik op **New** (Nieuw).

Hierna volgt een voorbeeld:



Wanneer het venster Profile Management (General) wordt weergegeven, voltooit u deze stappen om de Profile Name, Client Name en SSID te instellen:

Voer de naam van het profiel in het veld Profielnaam in.

Dit voorbeeld gebruikt **OFFICE** als de profielnaam.

Voer de naam van de client in het veld Naam client in.

De clientnaam wordt gebruikt om de draadloze client in het WLAN-netwerk te identificeren. Deze configuratie gebruikt de naam **Client 1** voor de eerste client.

Voer onder Netwerknamen de SSID in dat voor dit profiel moet worden gebruikt.

SSID is hetzelfde als SSID dat u in de AP hebt ingesteld. SSID in dit voorbeeld is **CISCO123**.

The image shows a screenshot of a 'Profile Management' dialog box with the 'Security' tab selected. The dialog has three tabs: 'General', 'Security', and 'Advanced'. It is divided into two main sections: 'Profile Settings' and 'Network Names'. In the 'Profile Settings' section, the 'Profile Name' field contains 'OFFICE' and the 'Client Name' field contains 'Client 1'. In the 'Network Names' section, the 'SSID1' field contains 'CISCO123', while 'SSID2' and 'SSID3' are empty. Red ovals highlight the 'Profile Name' and 'SSID1' fields. At the bottom right, there are 'OK' and 'Cancel' buttons.

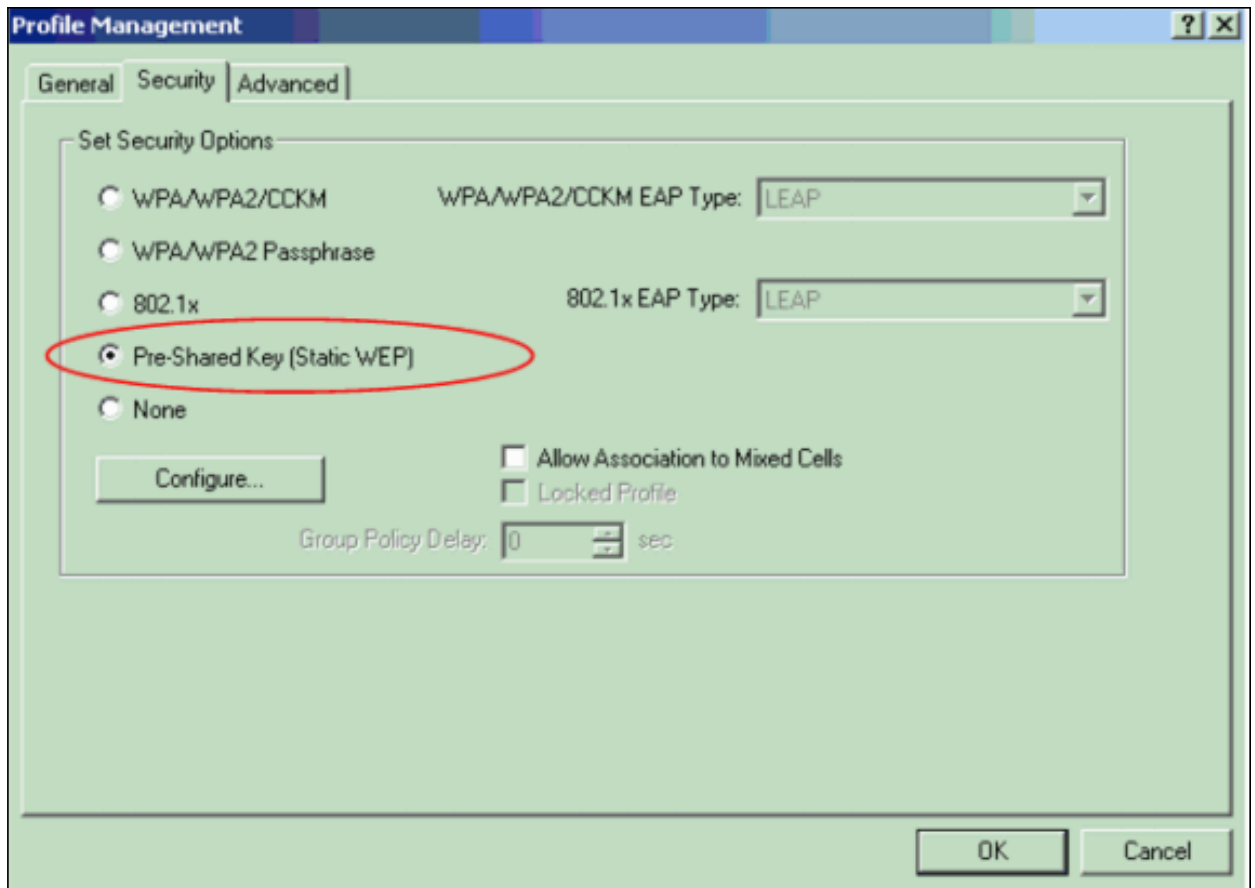
Field	Value
Profile Name	OFFICE
Client Name	Client 1
SSID1	CISCO123
SSID2	
SSID3	

Voltooi de volgende stappen om de beveiligingsopties in te stellen:

Klik op het tabblad **Beveiliging** boven in het venster.

Klik op **Vooraf gedeelde sleutel (Statische WLAN)** onder Instellen beveiligingsopties.

Hierna volgt een voorbeeld:

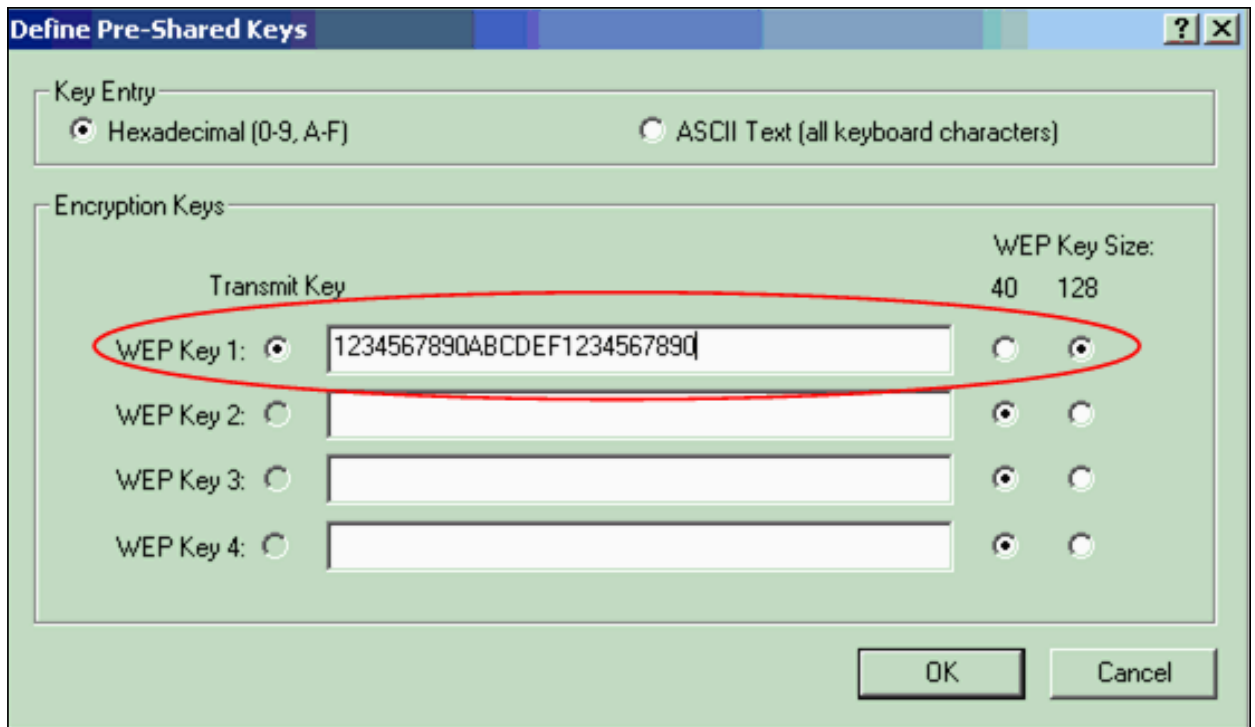


Klik op **Configureren**.

Het venster Vooraf gedeelde toetsen definiëren verschijnt.

Klik op een van de knoppen in het gebied Key Entry om een sleuteltype voor de invoer te kiezen.

Dit voorbeeld gebruikt **Hexadecimaal (0-9, A-F)**.



Voer onder Encryption Keys de sleutel van EFN in die voor encryptie van de gegevenspakketten moet worden gebruikt.

Dit voorbeeld gebruikt de sleutel van **1234567890abcdef1234567890**. Zie het voorbeeld in Stap d.

Opmerking: Gebruik dezelfde EFN-toets als de modus die u in het AP hebt ingesteld.

Klik op **OK** om de sleutel van de EVN op te slaan.

Voltooi deze stappen om de authenticatiemethode in te stellen op openen:

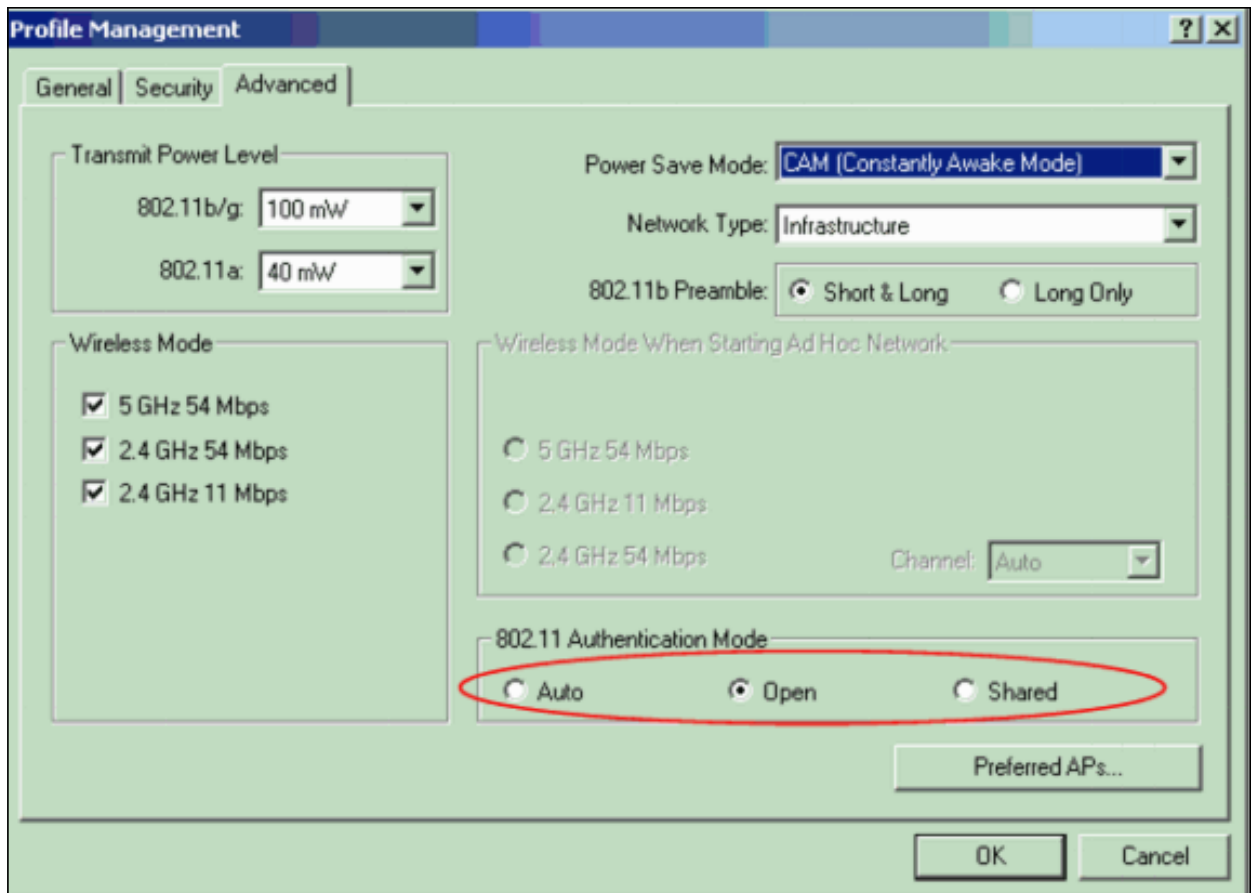
Klik op het tabblad **Geavanceerd** boven in het venster Profile Management.

Zorg ervoor dat **Open** is geselecteerd onder de verificatiemodus 802.11.

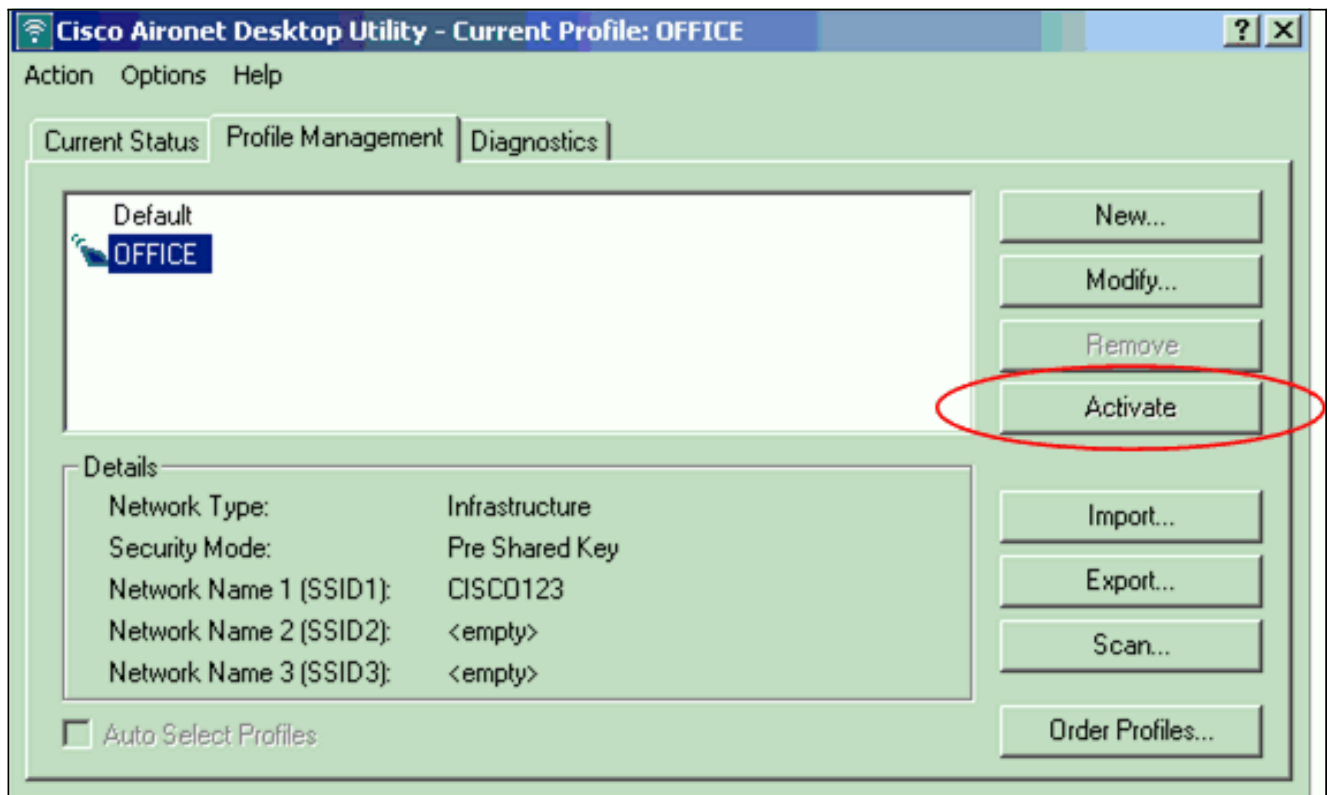
Opmerking: Open authenticatie is gewoonlijk standaard ingeschakeld.

Laat alle andere instellingen met de standaardwaarden zitten.

Klik op **OK**.



Klik op **Activeren** om dit profiel in te schakelen.



N.B.: U kunt deze zelfde [stap-voor-stap instructies](#) gebruiken om een volledig nieuw profiel te maken. In een alternatieve methode om een profiel te maken, scant de clientadapter de RF-omgeving om op beschikbare netwerken te controleren en maakt vervolgens een profiel op basis van de scanresultaten. Raadpleeg voor meer informatie over deze methode het gedeelte [Een](#)

[nieuw profiel maken van de Profile Manager.](#)

U kunt dezelfde procedure gebruiken om de twee andere clientadapters te configureren. U kunt dezelfde SSID op de andere adapters gebruiken. Het enige verschil is de naam van de client en het IP-adres dat statisch aan de adapter wordt gegeven.

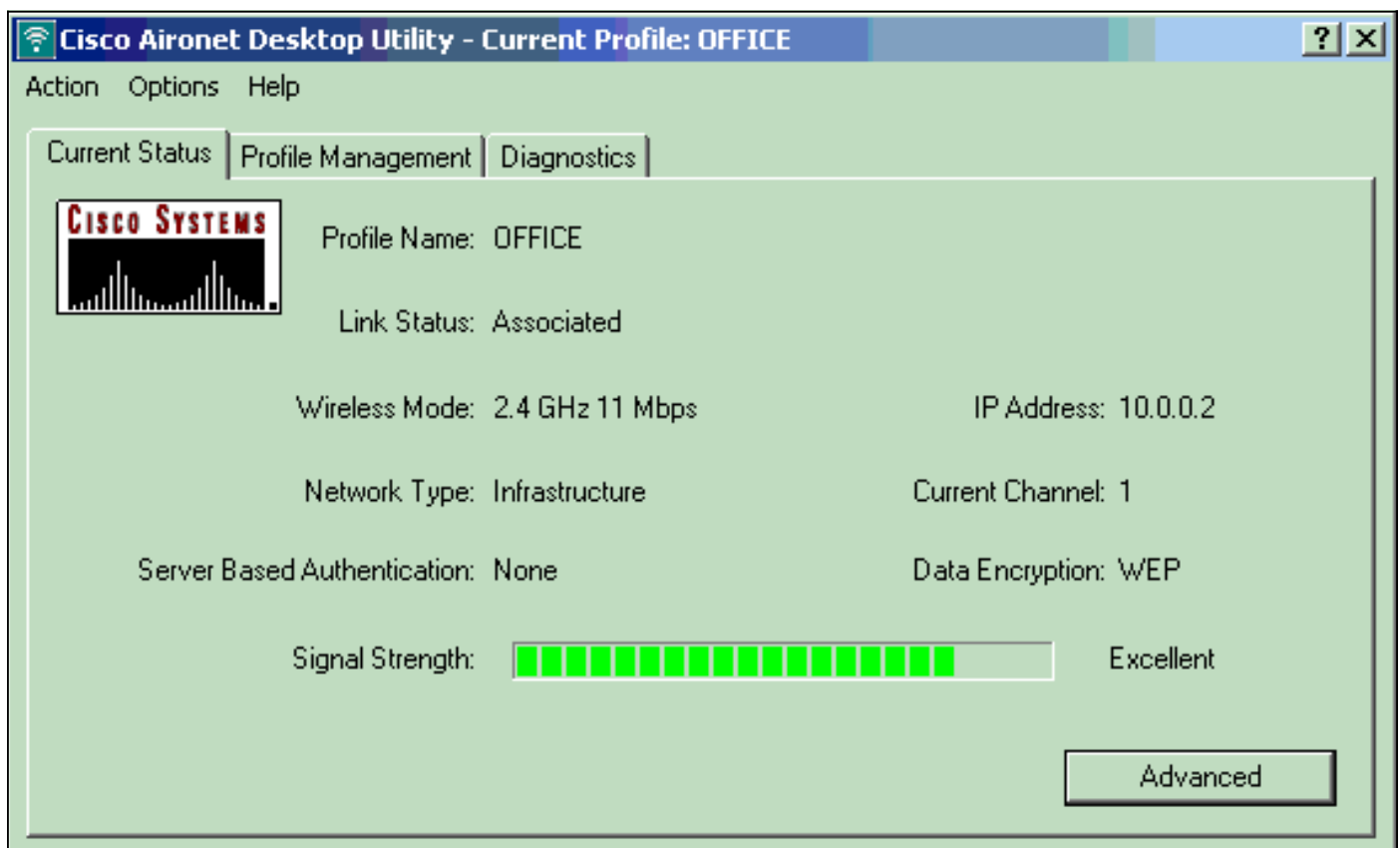
Opmerking: Dit voorbeeld veronderstelt dat het IP-adres van de clientadapter handmatig is ingesteld en in hetzelfde subnetwerk zit als het AP.

[Verifiëren](#)

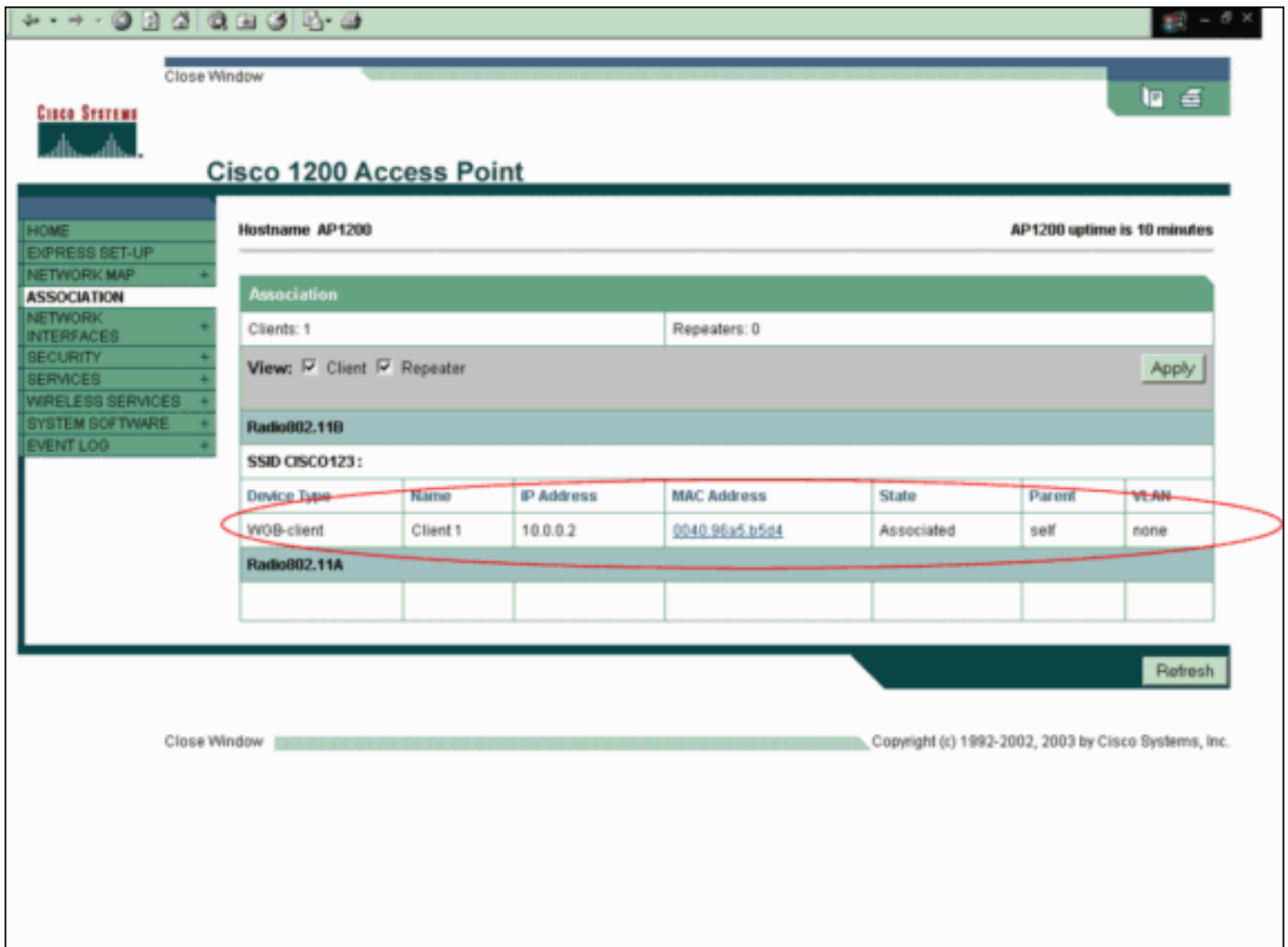
In dit gedeelte wordt uitgelegd hoe u kunt bevestigen dat de configuratie correct werkt.

Nadat u de configuraties hebt voltooid en het profiel hebt geactiveerd, sluit de clientadapter aan op de AP. Klik om de status van de clientverbinding te controleren op het tabblad **Huidige status** boven in het ADU-venster.

Dit voorbeeld illustreert een succesvolle verbinding met AP. U kunt zien dat de client Channel 1 gebruikt voor communicatie en dat de client gebruikmaakt van EFN voor codering. Aangezien alleen open verificatie wordt gebruikt, toont het veld Server-gebaseerde verificatie ook geen:



Als een andere methode om de clientverbinding op de AP te controleren, klikt u op **Associatie** in het menu links op de startpagina van AP. Hierna volgt een voorbeeld:



Problemen oplossen

Als 802.1x-verificatie wordt gebruikt en er een Cisco Catalyst 2950 of 3750 Switch in het netwerk aanwezig is, kan een 802.1X-client niet voor echt zijn. Deze foutmelding wordt weergegeven:

```
Jul 21 14:14:52.782 EDT: %RADIUS-3-ALLDEADSERVER: Group rad_eap:
No active radius servers found. Id 254
```

Dit symptoom wordt waargenomen op 2950 en 3750 Switches wanneer de waarden van de Staat van de RADIUS (24) tussen de Uitdaging van de Toegang en het Aanvraag van de Toegang veranderen. Dit komt door Cisco bug-id CSC50742. Dit wordt opgelost in Cisco IOS-software release 12.3(4)JA. Met release 12.3(4)JA vallen klanten niet langer onder 802.1X verificatie door Cisco Catalyst 2950 en 3750 Switches vanwege State (24) veldwaarden die veranderen.

Gerelateerde informatie

- [Cisco IOS-software release voor Cisco Aironet access points 12.3\(7\)BY](#)
- [Cisco Aironet 802.11a/b/g clientadapters voor draadloos LAN \(CB21AG en PI21AG\) installatie en configuratie Guide, OL-4211-04](#)
- [Het access point configureren voor het eerst](#)
- [Draadloze ondersteuningspagina](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)