

EAP-verificatie met WLAN-controllers (WLC) configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Configureren](#)

[Netwerkdigram](#)

[Het configureren van de WLC voor basisbediening en het registreren van de lichtgewicht AP's aan de controller](#)

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

[WLAN-parameters configureren](#)

[Cisco Secure ACS als de externe RADIUS-server configureren en een gebruikersdatabase voor verificatie maken](#)

[De client configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Tips bij het oplossen van problemen](#)

[EAP-timers manipuleren](#)

[Het pakketbestand via een ACS-RADIUS-server voor probleemoplossing ophalen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt uitgelegd hoe u de Wireless LAN controller (WLC) voor de MAP-verificatie (Extensible Authentication Protocol) kunt configureren met behulp van een externe RADIUS-server. Dit configuratievoorbeeld gebruikt de Cisco Secure Access Control Server (ACS) als de externe RADIUS-server om de gebruikersreferenties te valideren.

Voorwaarden

Vereisten

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

- Basiskennis van de configuratie van Lichtgewicht access points (APs) en Cisco WLCs.
- Basiskennis van Lichtgewicht AP Protocol (LWAPP).

- Kennis van hoe u een externe RADIUS-server kunt configureren zoals Cisco Secure ACS.

Gebruikte componenten

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

- Cisco Aironet 1232AG Series lichtgewicht AP
- Cisco 4400 Series WLC-software met firmware 5.1
- Cisco Secure ACS dat versie 4.1 ondersteunt
- Cisco Aironet 802.11a/b/g clientadapter
- Cisco Aironet Desktop Utility (ADU) die firmware 4.2 uitvoert

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.](#)

Configureren

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

N.B.: Gebruik het [Opdrachtuppgereedschap \(alleen geregistreeerde klanten\)](#) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Voltooi deze stappen om de toestellen voor MAP-verificatie te configureren:

1. [Configuratie van de WLC voor basisbediening en registratie van de lichtgewicht APs aan de controller.](#)
2. [Configureer de WLC voor RADIUS-verificatie via een externe RADIUS-server.](#)
3. [Configureer de WLAN-parameters.](#)
4. [Configureer Cisco Secure ACS als de externe RADIUS-server en maak een gebruikersdatabase voor het authenticeren van klanten.](#)

Netwerkdigram

In deze opstelling worden een Cisco 4400 WLC en een Lichtgewicht AP aangesloten door een hub. Een externe RADIUS-server (Cisco Secure ACS) is ook aangesloten op dezelfde hub. Alle apparaten zijn in hetzelfde net. Het AP is aanvankelijk geregistreerd bij de controller. U moet de WLC en AP configureren voor lichtgewicht uitgebreide Verificatieprotocol (LEAP). De klanten die verbinding maken met AP gebruiken LEAP authenticatie om te associëren met AP. Cisco Secure ACS wordt gebruikt om RADIUS-verificatie uit te voeren.



[Het configureren van de WLC voor basisbediening en het registreren van de lichtgewicht AP's aan de controller](#)

Gebruik de wizard opstartconfiguratie in de opdrachtregel-interface (CLI) om de WLC te configureren voor een eenvoudige bediening. In plaats hiervan kunt u ook de GUI gebruiken om de WLC te configureren. Dit document legt de configuratie op de WLC uit met de wizard opstarten in de CLI.

Nadat de WLC voor het eerst start, gaat het direct in de opstartconfiguratie wizard. Gebruik de configuratiewizard om basisinstellingen te configureren. U kunt de wizard op de CLI of de GUI uitvoeren. Deze uitvoer toont een voorbeeld van de opstartconfiguratiewizard in de CLI:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_33:84:a0]: WLC-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****
Management Interface IP Address: 10.77.244.204
Management Interface Netmask: 255.255.255.224
Management Interface Default Router: 10.77.244.220
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 4]: 1
Management Interface DHCP Server IP Address: 10.77.244.220
AP Manager Interface IP Address: 10.77.244.205
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.77.244.220):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Test
Network Name (SSID): Cisco123
Allow Static IP Addresses [YES][no]: yes
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
```

```
Configuration saved!
Resetting system with new configuration..
```

Met deze parameters wordt de WLC ingesteld voor een eenvoudige bediening. In dit configuratievoorbeeld gebruikt de WLC **10.77.244.204** als het IP-adres van de beheersinterface en **10.77.244.205** als het IP-adres van de AP-Manager.

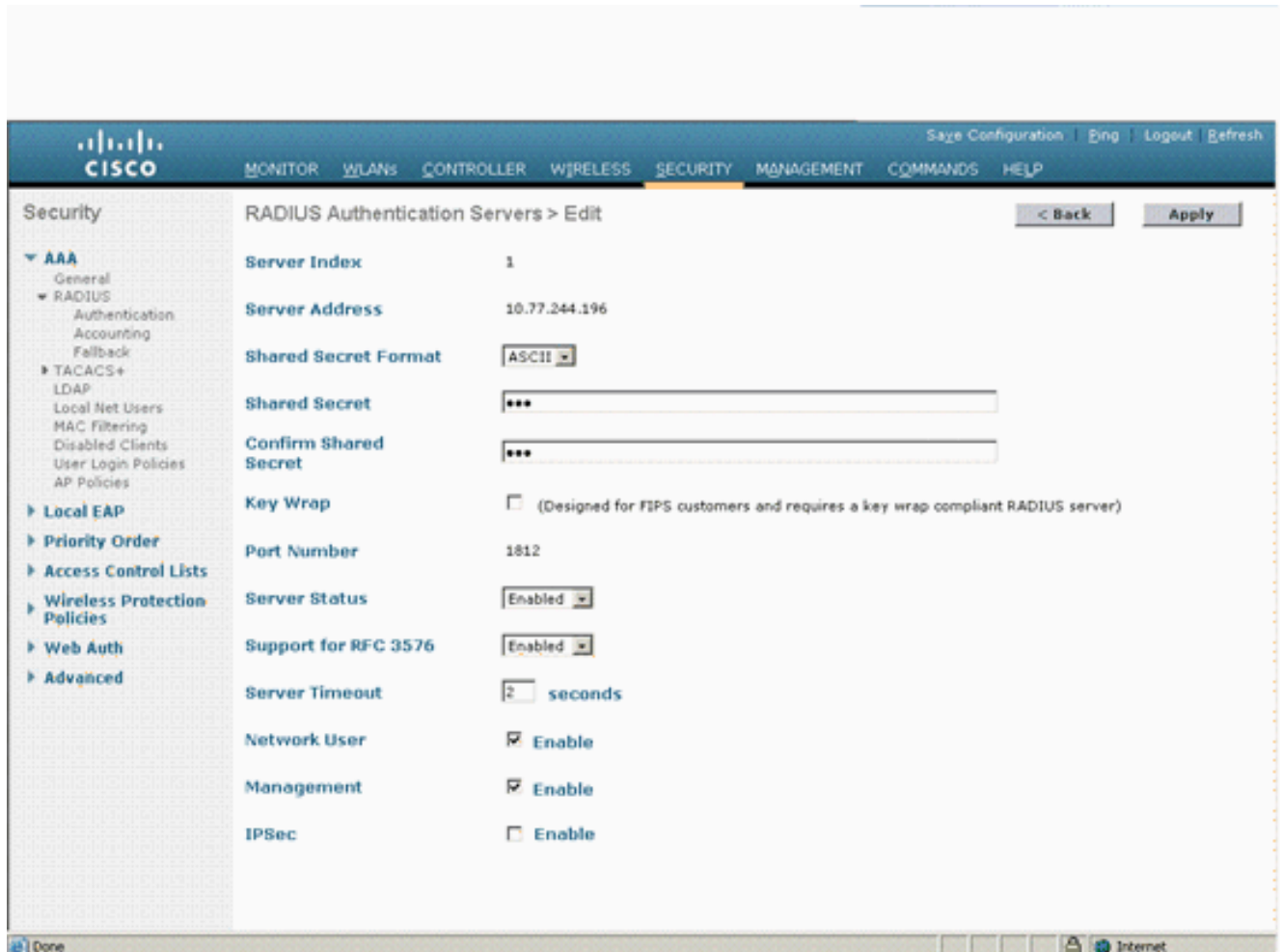
Voordat er andere functies op de WLC's kunnen worden ingesteld, moeten de lichtgewicht AP's zich registreren bij de WLC. Dit document gaat ervan uit dat de lichtgewicht AP bij de WLC is geregistreerd. Raadpleeg de [LAP-registratie \(Lichtgewicht AP\) bij een draadloze LAN-controller \(WLC\)](#) voor meer informatie over hoe de lichtgewicht AP's zich registreren bij de WLC.

Configureer de WLC voor RADIUS-verificatie met een externe RADIUS-server

De WLC moet worden geconfigureerd om de gebruikersreferenties naar een externe RADIUS-server te kunnen doorsturen. De externe RADIUS-server bevestigt vervolgens de gebruikersreferenties en geeft toegang tot de draadloze clients.

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

1. Kies **Security** en **RADIUS-verificatie** van de controller GUI om de pagina RADIUS-verificatieservers weer te geven. Klik vervolgens op **New** om een RADIUS-server te definiëren.



2. Definiëert de parameters van de RADIUS-server in de RADIUS-verificatieservers > Nieuwe pagina. Deze parameters omvatten het IP-adres van de RADIUS-server, gedeeld geheim, poortnummer en serverstatus. De controles van de Netwerkgebruiker en van het Beheer bepalen of de op RADIUS gebaseerde authenticatie van toepassing is voor WLC beheer en netwerkgebruikers. Dit voorbeeld gebruikt Cisco Secure ACS als de RADIUS-server met IP-adres 10.7.24.196.
3. Radius server kan nu door WLC voor authenticatie worden gebruikt. U kunt de lijst Radius Server vinden als u **Beveiliging > Straal > Verificatie** kiest.

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.77.244.196	1812	Disabled	Enabled

RFC 3576 wordt ondersteund op de RADIUS-server (CZS) van Cisco Access Registrar (CAR), maar niet op Cisco Secure ACS Server versie 4.0 en eerder. U kunt de lokale RADIUS-serverfunctie ook gebruiken om gebruikers voor authentiek te verklaren. Lokale RADIUS-server is geïntroduceerd met versie 4.1.17.0-code. WLC's die vorige versies draaien, hebben niet de functie met de lokale straal. Plaatselijke MAP is een authenticatiemethode die het mogelijk maakt dat gebruikers en draadloze klanten lokaal worden geauthentiseerd. Het is ontworpen voor gebruik in afgelegen kantoren die connectiviteit op draadloze klanten willen handhaven wanneer het backend systeem verstoord wordt of de externe authenticatieserver daalt. Plaatselijke MAP haalt gebruikersreferenties op uit de lokale gebruikersdatabase of de LDAP backend-database om gebruikers echt te maken. Lokale MAP ondersteunt LEAP, EAP-FAST met PAC's, EAP-FAST met certificaten en EAP-TLS-authenticatie tussen de controller en draadloze klanten. Plaatselijke MAP is ontworpen als een back - up - authenticatiesysteem. Als er RADIUS-servers zijn ingesteld op de controller, probeert de controller eerst de draadloze klanten te authenticeren met de RADIUS-servers. Plaatselijke MAP wordt alleen geprobeerd als er geen RADIUS-servers worden gevonden, hetzij omdat de RADIUS-servers zijn uitgelijnd, hetzij omdat er geen RADIUS-servers zijn ingesteld. Raadpleeg [Lokale EAP-verificatie op de draadloze LAN-controller met EAP-FAST- en LDAP-serverconfiguratie Voorbeeld](#) voor meer informatie over het configureren van lokale EAP op draadloze LAN-controllers.

[WLAN-parameters configureren](#)

Daarna moet u de WLAN-functie configureren die de clients gebruiken om verbinding te maken met het draadloze netwerk. Wanneer u de basisparameters voor de WLC hebt ingesteld, hebt u ook de SSID voor de WLAN ingesteld. U kunt deze SSID voor WLAN gebruiken of een nieuwe SSID maken. In dit voorbeeld maakt u een nieuwe SSID.

Opmerking: U kunt maximaal zestien WLAN's op de controller configureren. De Cisco WLAN-oplossing kan maximaal 16 WLAN's controleren voor lichtgewicht AP's. Elk WLAN kan worden toegewezen aan een uniek beveiligingsbeleid. Lichtgewicht AP's zenden alle actieve WLAN-oplossing van Cisco uit en voeren het beleid af dat u voor elke WLAN definieert.

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

1. Klik op **WLAN's** vanuit de GUI van de controller om de WLAN's pagina weer te geven. Deze pagina toont de WLAN's die op de controller bestaan.
2. Kies **Nieuw** om een nieuw WLAN te maken. Voer de naam van het profiel en de WLAN-sid in

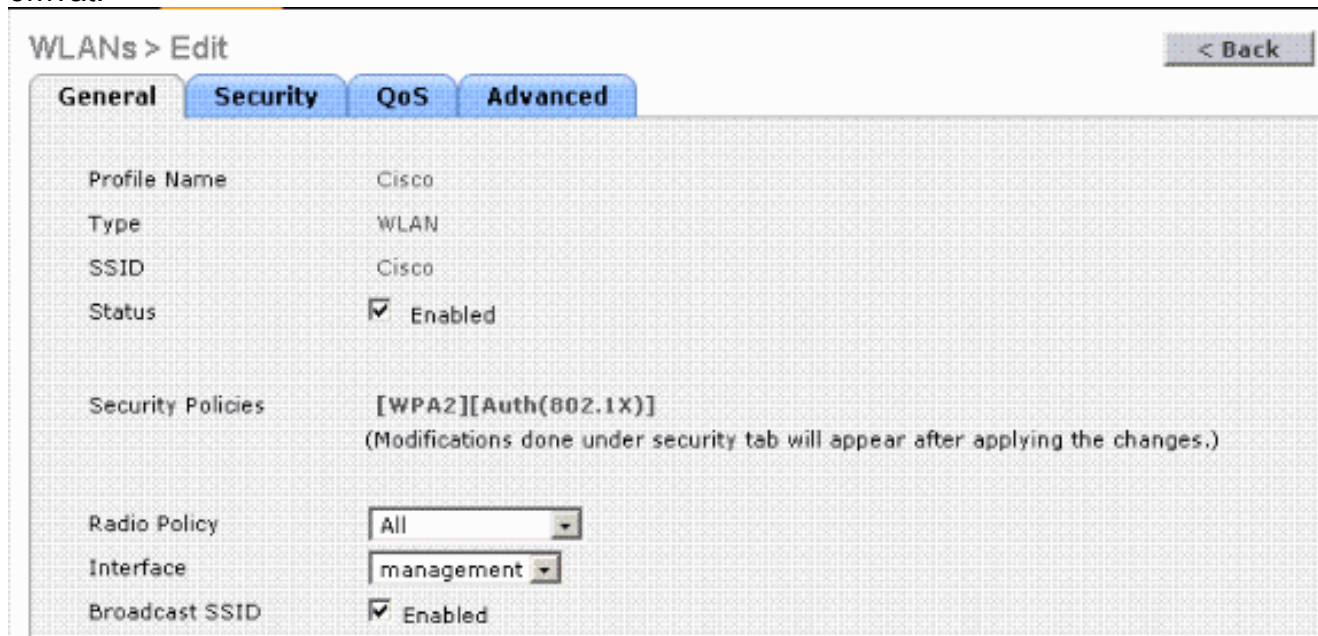
voor WLAN en klik op **Toepassen**. Dit voorbeeld gebruikt Cisco als SSID.



The screenshot shows the Cisco configuration interface for creating a new WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The 'WLANs' section is active, showing a breadcrumb 'WLANs > New'. The configuration fields are as follows:

Type	WLAN
Profile Name	Cisco
WLAN SSID	Cisco

3. Zodra u een nieuw WLAN hebt gemaakt, wordt de WLAN > Pagina-bewerken voor het nieuwe WLAN weergegeven. In deze pagina kunt u verschillende parameters definiëren die specifiek zijn voor dit WLAN, dat algemeen beleid, beveiligingsbeleid, QoS-beleid en andere geavanceerde parameters omvat.

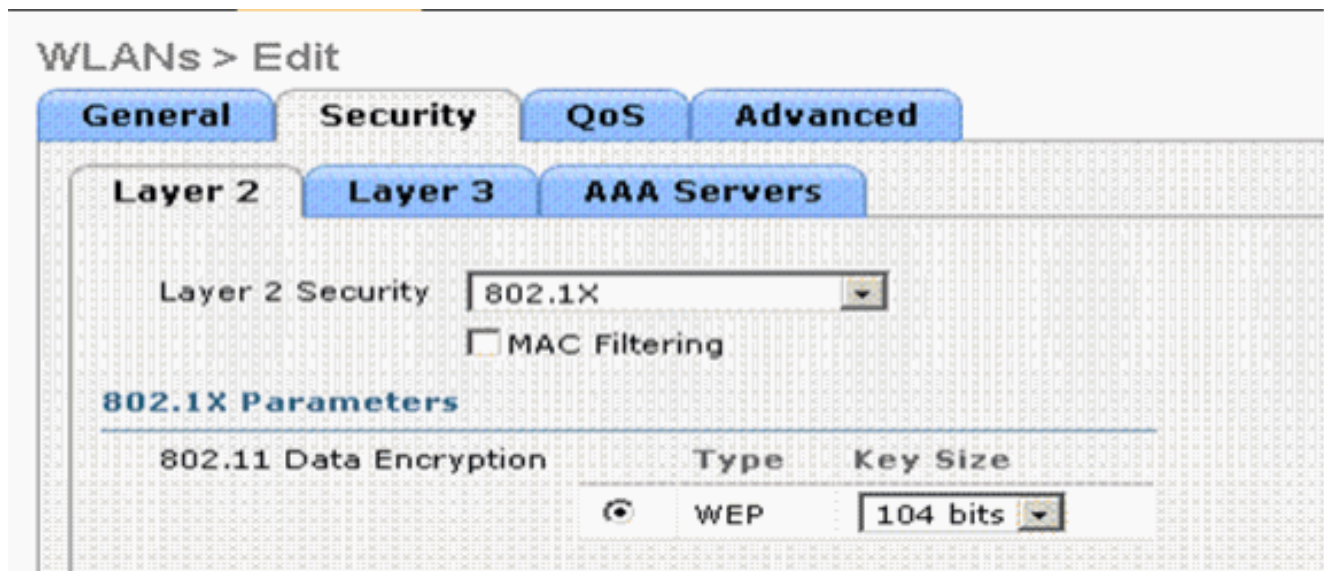


The screenshot shows the 'WLANs > Edit' configuration page. The 'Security' tab is selected. The configuration fields are as follows:

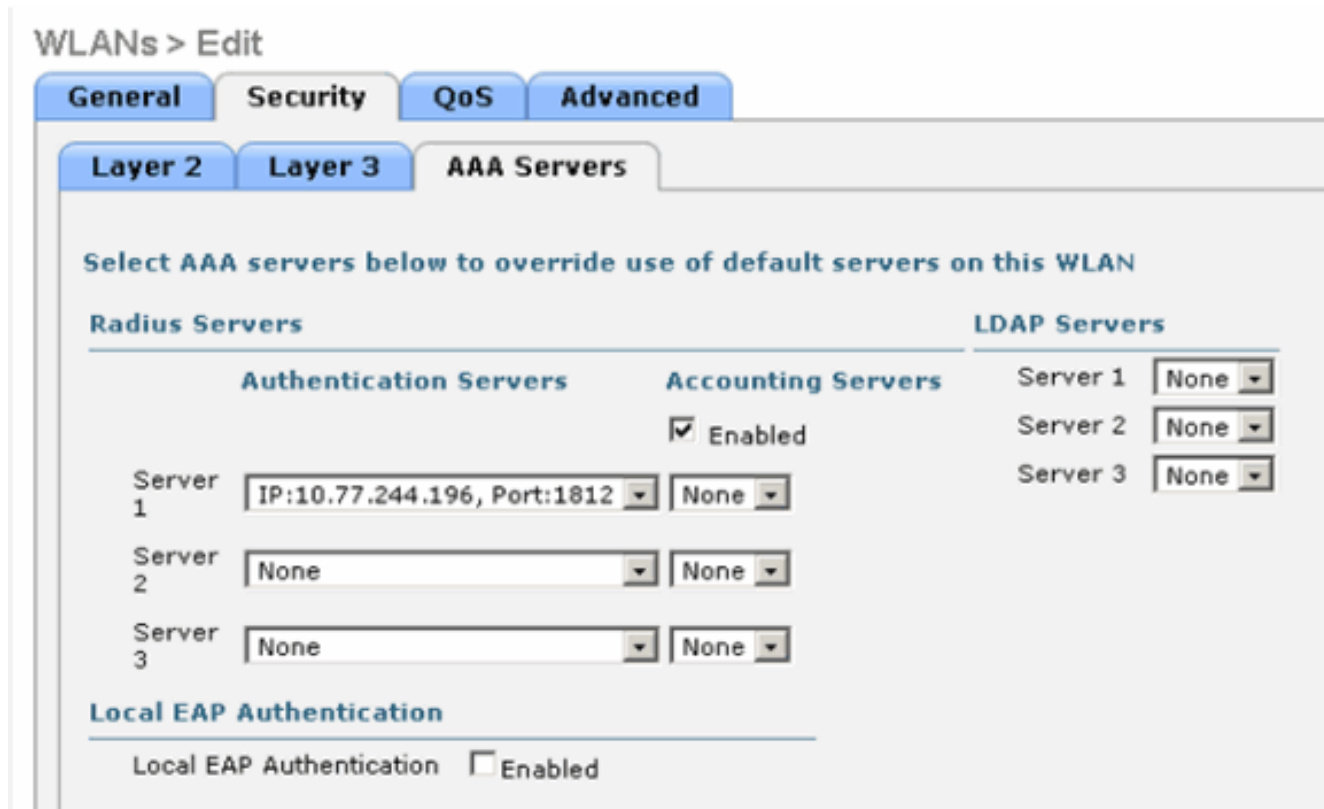
Profile Name	Cisco
Type	WLAN
SSID	Cisco
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Kies de juiste interface in het vervolgkeuzemenu. De andere parameters kunnen worden gewijzigd op basis van de vereisten van het WLAN-netwerk. Controleer de **status** onder Algemeen beleid om het WLAN in te schakelen.

4. Klik op het tabblad **Security** en kies **Layer 2 Security**. Kies in het vervolgkeuzemenu Layer 2 Security de optie **802.1x**. In de parameters 802.1x kiest u de grootte van de sleutel. In dit voorbeeld wordt gebruik gemaakt van de 128-bits-sleutel, de 104-bits-sleutel plus de 24-bits Initialisatiedrager.



5. Kies het tabblad **AAA-servers**. Kies in het uitrolmenu Verificatieservers (RADIUS) de juiste RADIUS-server. Deze server wordt gebruikt om de draadloze clients te authenticeren.

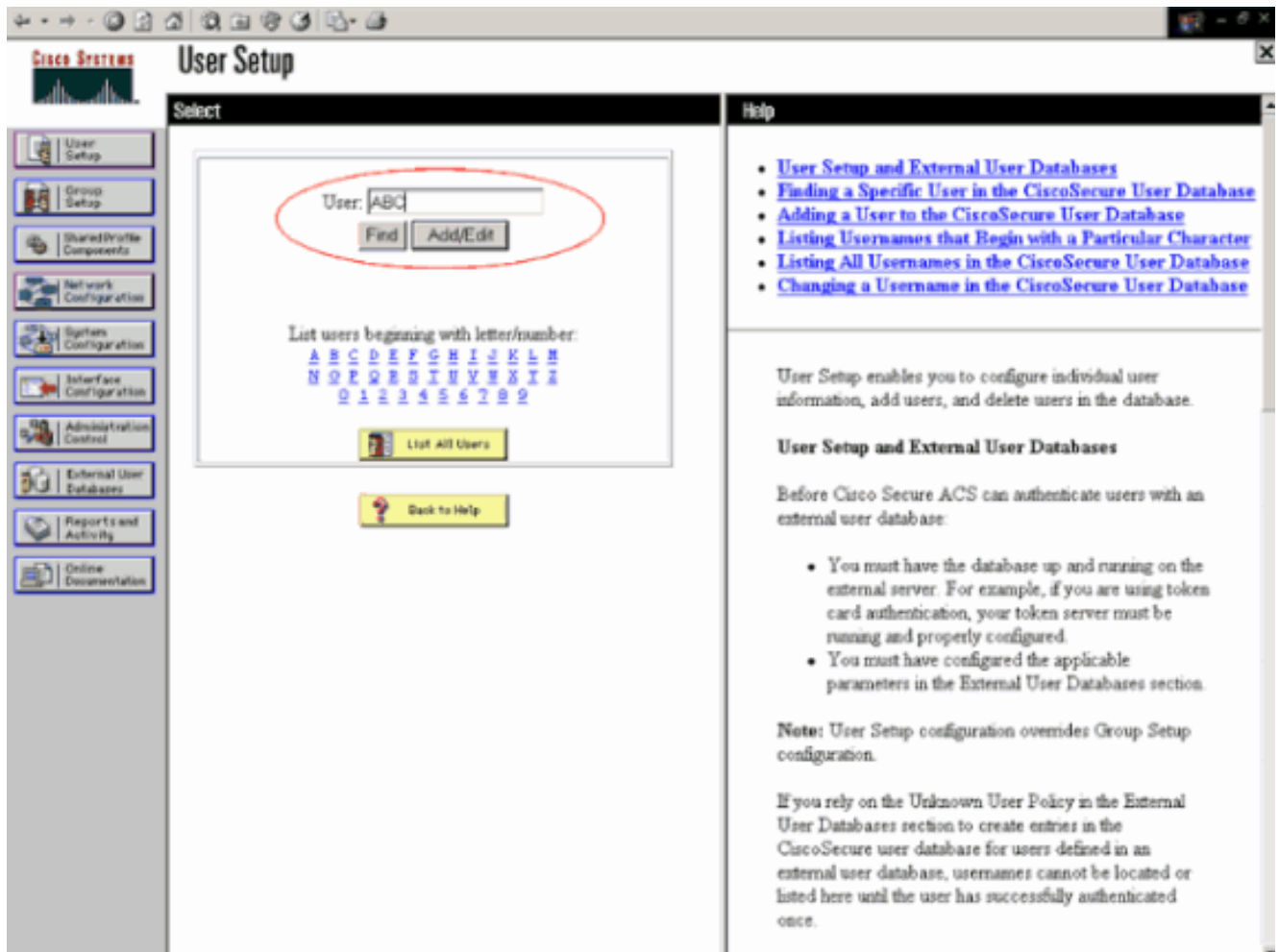


6. Klik op **Toepassen** om de configuratie op te slaan.

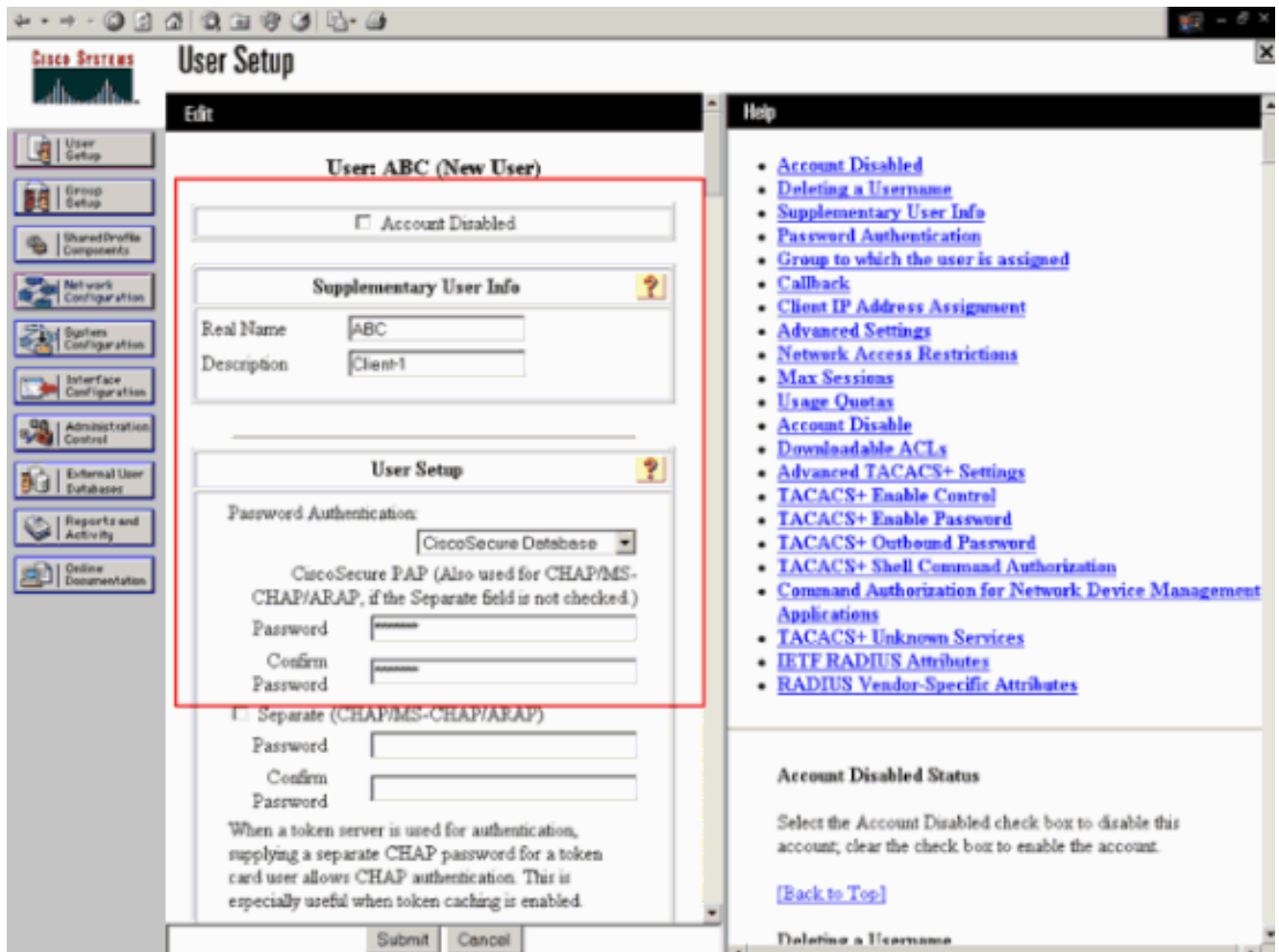
[Cisco Secure ACS als de externe RADIUS-server configureren en een gebruikersdatabase voor verificatie maken](#)

Voltooi deze stappen om de gebruikersdatabase te maken en EAP-verificatie op de Cisco Secure ACS mogelijk te maken:

1. Klik op **Gebruikersinstelling** in de ACS GUI, voer de gebruikersnaam in en klik op **Toevoegen/Bewerken**. In dit voorbeeld is de gebruiker **ABC**.



2. Wanneer de pagina Gebruikersinstellingen verschijnt, definieert u alle parameters die specifiek zijn voor de gebruiker. In dit voorbeeld worden de gebruikersnaam, het wachtwoord en de aanvullende gebruikersinformatie ingesteld omdat u deze parameters alleen nodig hebt voor MAP-verificatie. Klik op **Indienen** en herhaal hetzelfde proces om meer gebruikers aan de database toe te voegen. Standaard worden alle gebruikers gegroepeerd onder de standaardgroep en krijgen ze hetzelfde beleid toegewezen als dat voor de groep is gedefinieerd. Raadpleeg het gedeelte [Gebruikersgroep Management](#) van de [gebruikersgids voor Cisco Secure ACS voor Windows Server 3.2](#) voor meer informatie als u specifieke gebruikers aan verschillende groepen wilt toewijzen.

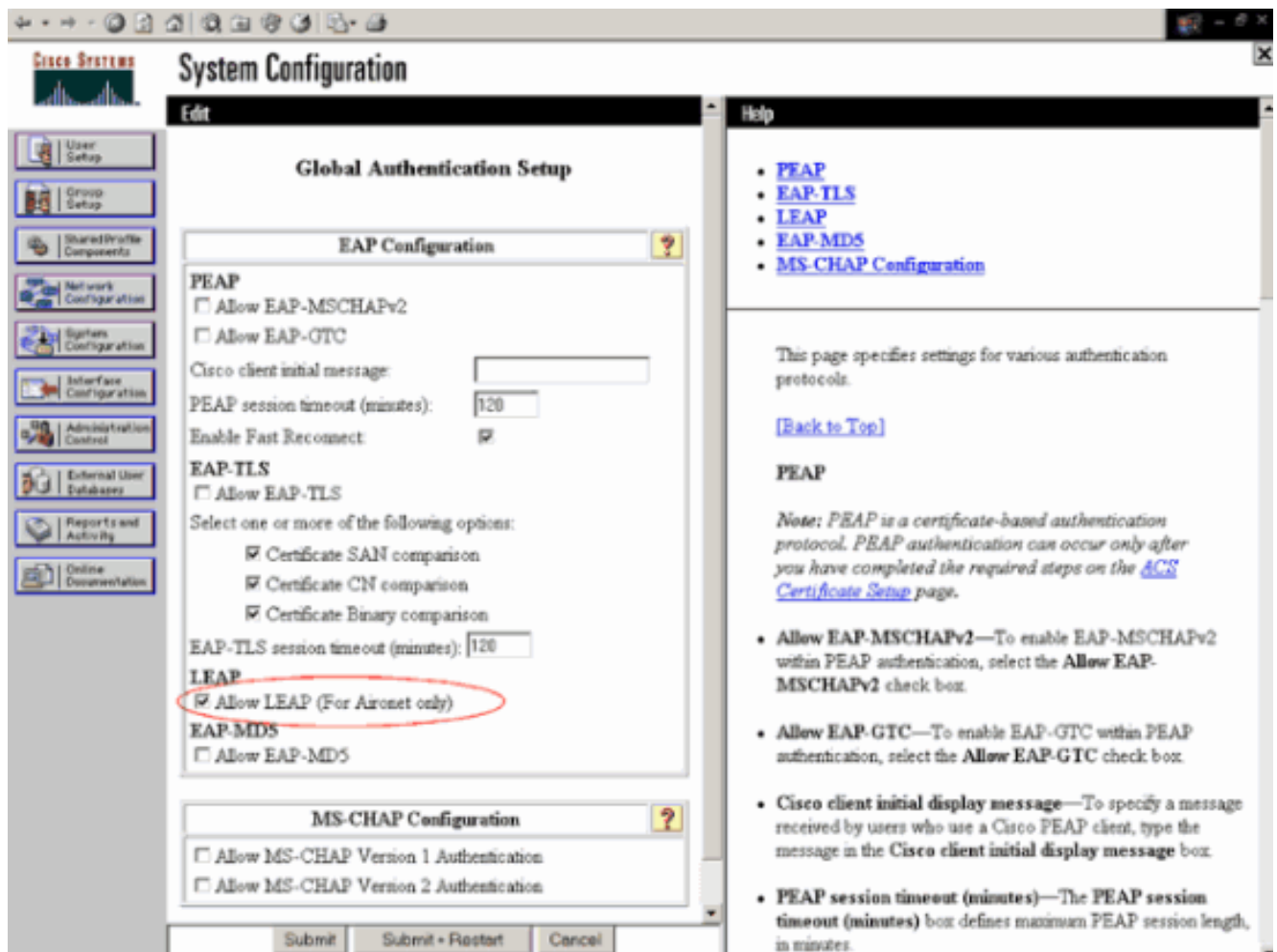


3. Definiert de controller als een AAA-client op de ACS-server. Klik op **Netwerkconfiguratie** vanuit de ACS-GUI. Wanneer de pagina Network Configuration verschijnt, specificiert u de naam van de WLC, IP-adres, gedeelde geheime en verificatiemethode (RADIUS Cisco Airespace). Raadpleeg de documentatie van de fabrikant voor andere niet-ACS-verificatieservers. **Opmerking:** de gedeelde geheime sleutel die u op de WLC en de ACS server vormt moet overeenkomen. Het gedeelde geheim is hoofdlettergevoelig.

Add AAA Client

AAA Client Hostname	<input type="text" value="WLC-1"/>
AAA Client IP Address	<input type="text" value="10.77.244.204"/>
Shared Secret	<input type="text" value="cisco"/>
<hr/>	
RADIUS Key Wrap	
Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<input type="radio"/> ASCII <input checked="" type="radio"/> Hexadecimal
<hr/>	
Authenticate Using	<input type="text" value="RADIUS (Cisco Airespace)"/>
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure)	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	
<input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client	
<input type="checkbox"/> Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	

4. Klik op **System Configuration** en **Global Authentication Setup** om te verzekeren dat de verificatieserver is ingesteld voor het uitvoeren van de gewenste MAP-verificatiemethode. Kies in de MAP-configuratie de juiste MAP-methode. In dit voorbeeld wordt gebruik gemaakt van MAP-authenticatie. Klik op **Inzenden** als u klaar bent.

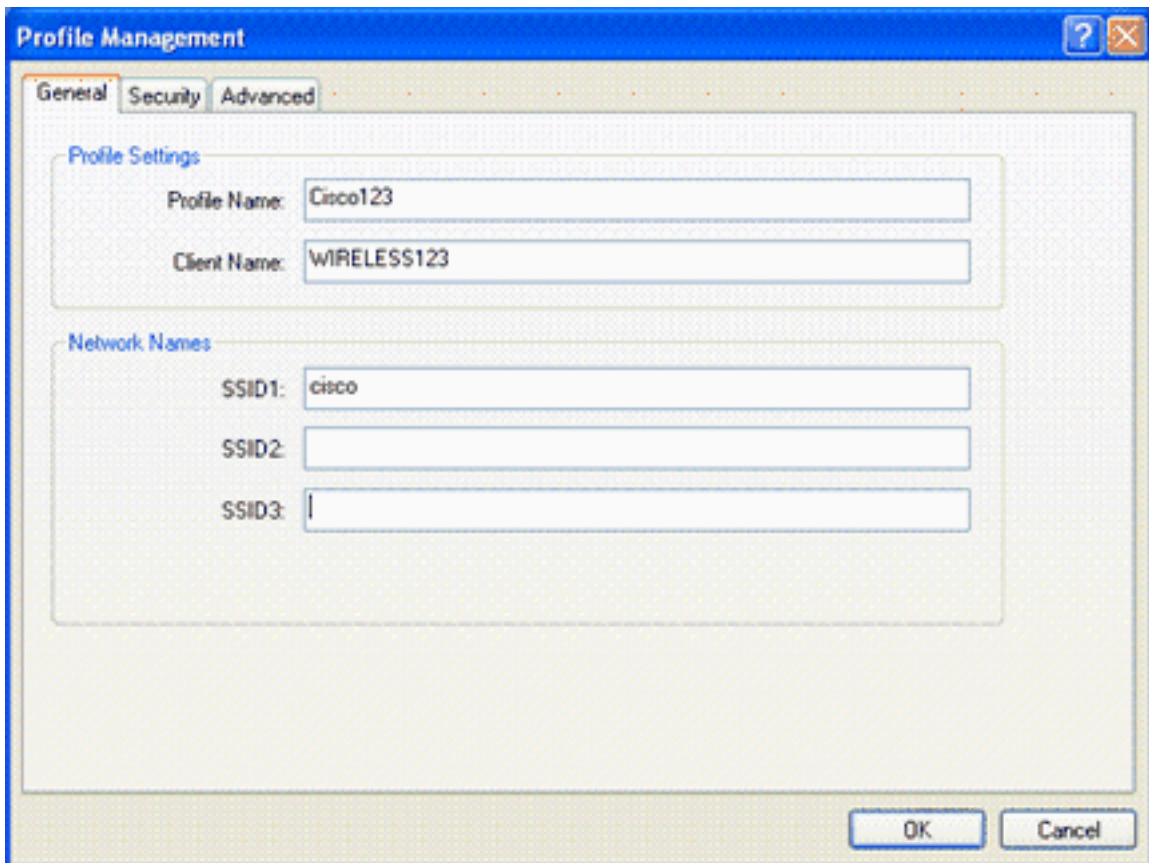


[De client configureren](#)

De klant moet ook voor het juiste MAP-type worden ingesteld. De klant stelt het MAP-type voor aan de server tijdens het MAP-onderhandelingsproces. Als de server dat MAP-type ondersteunt, erkent hij het MAP-type. Indien het MAP-type niet wordt ondersteund, wordt er een negatieve bevestiging verzonden en onderhandelt de cliënt opnieuw met een andere MAP-methode. Dit proces duurt voort totdat over een ondersteund MAP-type is onderhandeld. In dit voorbeeld wordt LEAP als MAP-type gebruikt.

Voltooi deze stappen om LEAP op de client te configureren met Aironet desktop Utility.

1. Dubbelklik op het pictogram **Aironet Utility** om het te openen.
2. Klik op het tabblad **Profielbeheer**.
3. Klik op een profiel en kies **Wijzigen**.
4. Kies onder het tabblad Algemeen een *profielnaam*. Voer de **SSID** van de WLAN

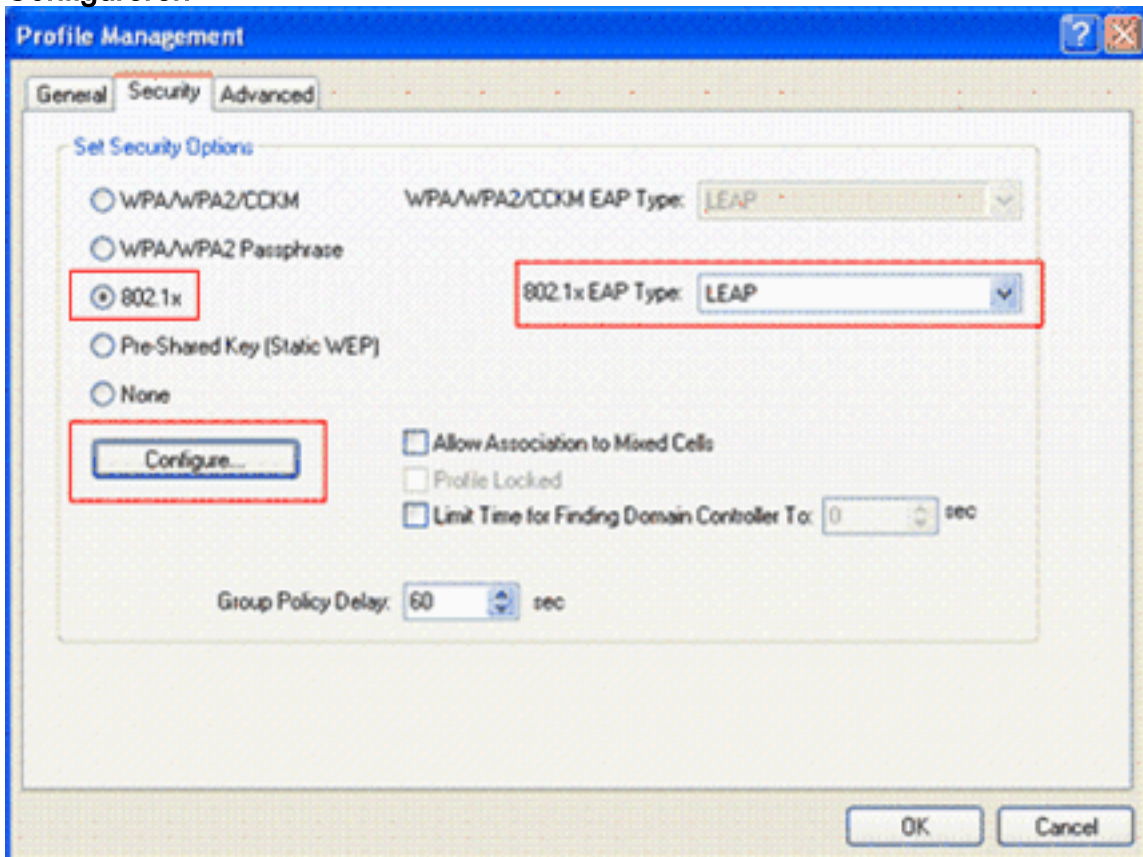


in.

Opmerki

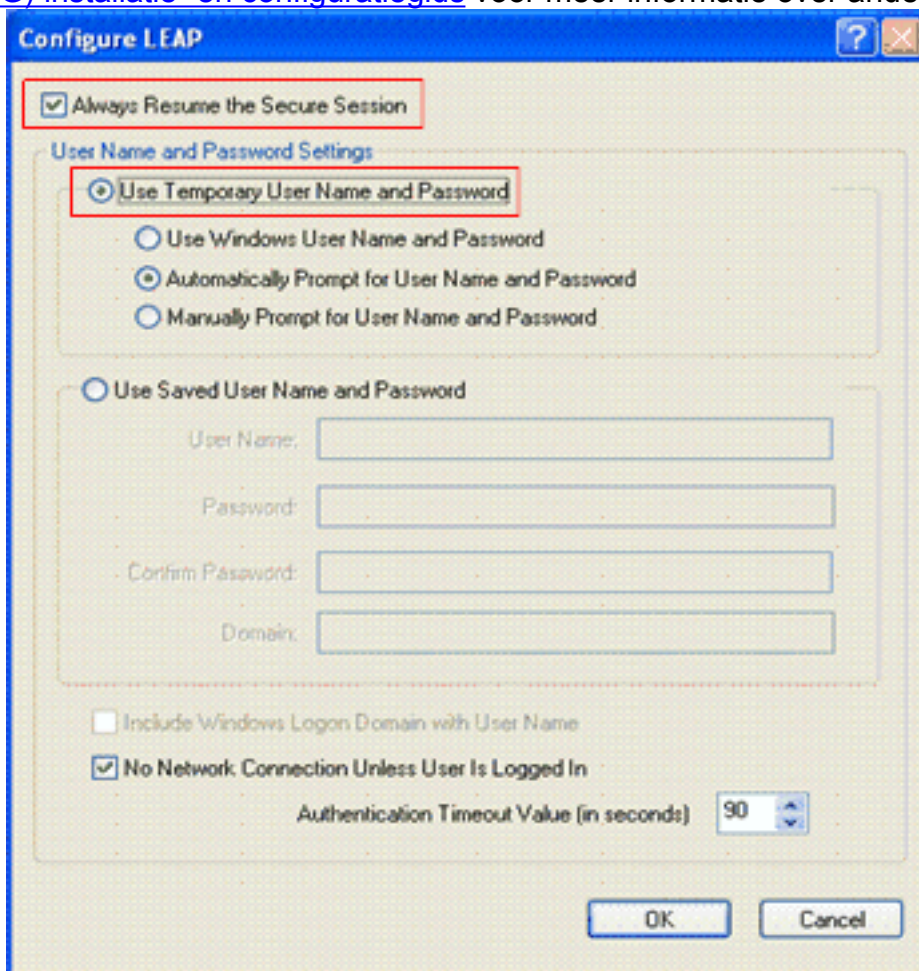
ng: SSID is hoofdlettergevoelig en moet exact overeenkomen met de SSID die op de WLC is ingesteld.

5. Kies onder het tabblad **Security** 802.1x. Kies het MAP-type als **LEAP** en klik op **Configureren**.



6. Kies **Gebruik tijdelijke gebruikersnaam en wachtwoord**, wat u ertoe aanzet om de gebruikershandleiding elke keer als u de computer opnieuw start in te voeren. Controleer een van de drie hier gegeven opties. In dit voorbeeld wordt **automatisch** gevraagd naar

gebruikersnaam en wachtwoord. Daarvoor is het nodig dat u de *LEAP*-gebruikersreferenties invoert naast de *Windows-naam en het wachtwoord* voordat u inlogt bij Windows. Schakel het aanvinkvakje Beveiligde sessie **altijd opnieuw** in bovenin het venster als u wilt dat de MAP-smeekbede altijd probeert de vorige sessie te hervatten zonder dat u hoeft te vragen om uw geloofsbrieven opnieuw in te voeren wanneer de clientadapter beweegt en zich opnieuw aan het netwerk associeert. **N.B.:** Raadpleeg het [gedeelte Clientadapter configureren](#) van het document [Cisco Aironet 802.11a/b/g clientadapters voor draadloos LAN \(CB21AG en PI21AG\) installatie- en configuratiegids](#) voor meer informatie over andere



opties.

7. Onder het tabblad **Advanced** kunt u de preamble, Aironet-extensie en andere 802.11-opties configureren, zoals Aan/uit, Frequentie enzovoort.
8. Klik op **OK**. De client probeert nu te associëren met de ingestelde parameters.

Verifiëren

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

Probeer een draadloze client met de lichtgewicht AP te associëren met behulp van LEAP-verificatie om te controleren of de configuratie werkt zoals verwacht.

Opmerking: In dit document wordt ervan uitgegaan dat het clientprofiel is ingesteld voor LEAP-verificatie. Raadpleeg het [gebruik van EAP-verificatie](#) voor meer informatie over het configureren van de 802.11a/b/g draadloze clientadapter voor LEAP-verificatie.

Nadat het profiel voor de draadloze client is geactiveerd, wordt de gebruiker gevraagd de gebruikersnaam/het wachtwoord voor LEAP-verificatie te verstrekken. Hierna volgt een voorbeeld:

Enter Wireless Network Password [X]

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 : EAP-Authentication

Lichtgewicht AP en dan geeft WLC de gebruikersgeloofsbrieven aan de externe server van de RADIUS (Cisco Secure ACS) door om de geloofsbrieven te valideren. De RADIUS-server vergelijkt de gegevens met de gebruikersdatabase en geeft toegang tot de draadloze client wanneer de gebruikersreferenties geldig zijn om de gebruikersreferenties te controleren. Het Passed Authentication-rapport op de ACS-server toont aan dat de client de RADIUS-verificatie heeft doorlopen. Hierna volgt een voorbeeld:

The screenshot shows the Cisco Reports and Activity page. On the left is a navigation menu with categories like User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Database, Reports and Activity, and Online Documentation. The main content area is titled 'Reports and Activity' and contains a list of reports such as TACACS+ Accounting, RADIUS Accounting, VoIP Accounting, Passed Authentications, Failed Attempts, Logged-in Users, Disabled Accounts, ACS Backup And Restore, Administration Audit, User Password Changer, and ACS Service Monitoring. A 'Back to Help' button is also visible.

The 'Passed Authentications active.csv' table contains the following data:

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAS-Port	NAS-IP-Address
04/04/2006	15:01:33	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30
04/04/2006	15:00:37	Authen OK	ABC	Default Group	00-40-96-AC-E6-57	1	172.16.1.30

Bij succesvolle RADIUS-verificatie associeert de draadloze client met de lichtgewicht AP.

The screenshot shows the 'LEAP Authentication Status' dialog box. It displays the following information:

- Card Name: Cisco Aironet 802.11 a/b/g Wireless Adapter
- Profile Name: EAP-Authentication

The authentication steps and their status are as follows:

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

At the bottom, there is a checkbox labeled 'Show minimized next time' and a 'Cancel' button.

Dit kan ook worden gecontroleerd onder het tabblad **Monitor** van de WLC GUI. Kies **monitor** > **Clients** en controleer voor het MAC-adres van de client.

Save Configuration | Ping | Logout | Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor

Summary

Statistics

Controller

Ports

Wireless

Rogue APs

Known Rogue APs

Rogue Clients

Adhoc Rogues

802.11a Radios

802.11b/g Radios

Clients

RADIUS Servers

Clients

Items 1 to 1 of 1

Search by MAC address Search

Client MAC Addr	AP Name	AP MAC Addr	WLAN	Type	Status	Auth	Port	
00:40:96:ac:e6:57	ap:5b:fb:d0	00:0b:85:5b:fb:d0	Cisco123	802.11a	Associated	Yes	1	Detail Link Test Disable Banlist

Problemen oplossen

Voltooi deze stappen om de configuraties met problemen op te lossen:

1. Gebruik de **debug lwapp gebeurtenissen** om opdracht te controleren of het AP zich bij de WLC registreert.
2. Controleer of de RADIUS-server de verificatieaanvraag van de draadloze client ontvangt en bevestigt. Controleer het NAS-IP-adres, de datum en de tijd om te controleren of de WLC de Radius-server heeft kunnen bereiken. Controleer de Geautomatiseerde verificaties en mislukte meldingen op de ACS-server om dit te bereiken. Deze verslagen zijn beschikbaar onder Rapporten en Activiteiten op de ACS-server. Hier is een voorbeeld wanneer de RADIUS-serververificatie faalt:

Cisco Systems

Reports and Activity

Select

Refresh Download

Failed Attempts active.csv

Date	Time	Message Type	User Name	Group Name	Caller ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port	NAS-IP-Address
04/04/2006	15:42:51	Authen failed	code		00-40-96-AC-E6-57	CS user unknown			1	172.16.1.30

Back to help

Opmerking: Raadpleeg [Verkennde versie en AAA Debug Informatie voor Cisco Secure ACS voor Windows](#) voor informatie over hoe u problemen kunt oplossen en debug informatie over Cisco Secure ACS kunt verkrijgen.

3. U kunt deze **debug**-opdrachten ook gebruiken om AAA-verificatie in te willigen:**debug in alle** schakelt u het debug van alle AAA-berichten in.**bug dot1x-pakket activeren**-schakelt het debug van alle punt1x-pakketten in.Hier is een voorbeelduitvoer van **debug 802.1x om opdracht toe te voegen:**

```
(Cisco Controller) >debug dot1x aaa enable
```

```
*Sep 23 15:15:43.792: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.793: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=11
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 AAA EAP Packet created request =
0x1533a288.. !!!!
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2, length=8,
id=2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.794: 00000000: 02 02 00 08 01 41 42 43
.....ABC
*Sep 23 15:15:43.794: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
Response'
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Received EAP Attribute (code=1,
length=19,id=3, dot1xcb->id = 2) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.799: 00000000: 01 03 00 13 11 01 00 08 42 3a 8e d1 18 24 e8 9f
.....B:...
*Sep 23 15:15:43.799: 00000010: 41 42 43
ABC
*Sep 23 15:15:43.799: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
00:40:96:ac:dd:05
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
index=1
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
index=2
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
index=5
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.901: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
```

```

*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.902: 00:40:96:ac:dd:05 Sending EAP Attribute (code=2,
    length=35, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.902: 00000000: 02 03 00 23 11 01 00 18 83 f1 5b 32 cf 65 04 ed
    ...#.....[2.e..
*Sep 23 15:15:43.902: 00000010: da c8 4f 95 b4 2e 35 ac c0 6b bd fa 57 50 f3 13
    ..O...5..k..WP..
*Sep 23 15:15:43.904: 00000020: 41 42 43
    ABC
*Sep 23 15:15:43.904: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Interim
    Response'
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 AAA Message 'Interim Response' received
    for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Received EAP Attribute (code=3,
    length=4,id=3, dotlxcb->id = 3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.907: 00000000: 03 03 00 04
    ....
*Sep 23 15:15:43.907: 00:40:96:ac:dd:05 Skipping AVP (0/80) for mobile
    00:40:96:ac:dd:05
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_USER_NAME(1) index=0
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLING_STATION_ID(31)
    index=1
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_CALLED_STATION_ID(30)
    index=2
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT(5) index=3
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IP_ADDRESS(4) index=4
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_IDENTIFIER(32)
    index=5
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_VAP_ID(1) index=6
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_SERVICE_TYPE(6) index=7
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_FRAMED_MTU(12) index=8
*Sep 23 15:15:43.912: 00:40:96:ac:dd:05 Adding AAA_ATT_NAS_PORT_TYPE(61) index=9
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_EAP_MESSAGE(79) index=10
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_RAD_STATE(24) index=11
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Adding AAA_ATT_MESS_AUTH(80) index=12
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 AAA EAP Packet created request =
    0x1533a288.. !!!!
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 Sending EAP Attribute (code=1,
    length=19, id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.915: 00000000: 01 03 00 13 11 01 00 08 29 23 be 84 e1 6c d6 ae
    .....)#...l..
*Sep 23 15:15:43.915: 00000010: 41 42 43
    ABC
*Sep 23 15:15:43.915: 00:40:96:ac:dd:05 [BE-req] Sending auth request to
    'RADIUS' (proto 0x140001)
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] AAA response 'Success'
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 [BE-resp] Returning AAA response
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 AAA Message 'Success' received for
    mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[0]: attribute 8,
    vendorId 0, valueLen 4
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[1]: attribute 79,
    vendorId 0, valueLen 35
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 Received EAP Attribute (code=2,
    length=35,id=3) for mobile 00:40:96:ac:dd:05
*Sep 23 15:15:43.918: 00000000: 02 03 00 23 11 01 00 18 03 66 2c 6a b3 a6 c3 4c
    ...#.....f,j...L
*Sep 23 15:15:43.918: 00000010: 98 ac 69 f0 1b e8 8f a2 29 eb 56 d6 92 ce 60 a6
    ..i.....).V...`.
*Sep 23 15:15:43.918: 00000020: 41 42 43

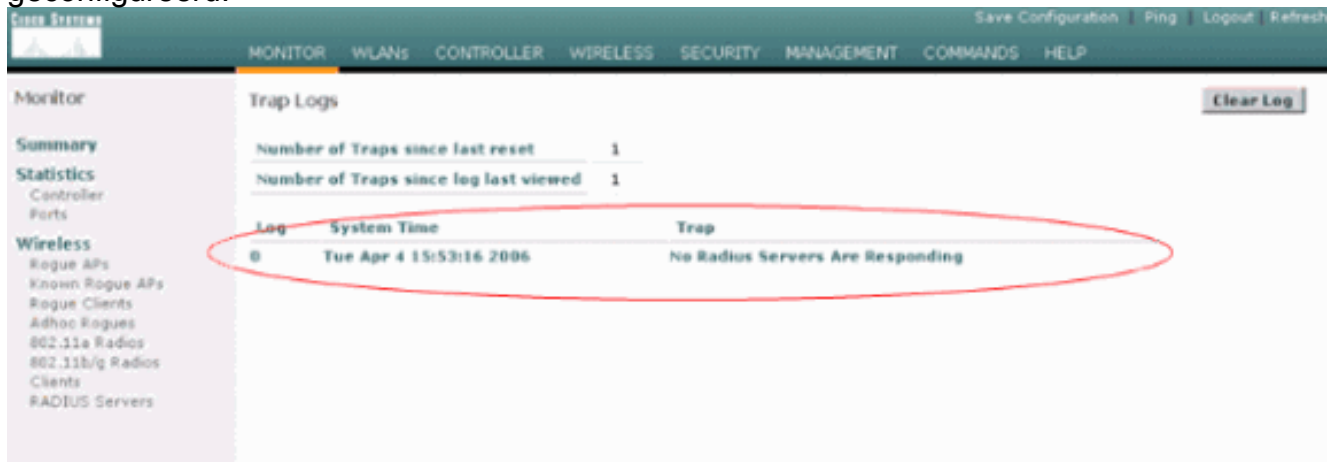
```

ABC

```
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[2]: attribute 1,
  vendorId 9, valueLen 16
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[3]: attribute 25,
  vendorId 0, valueLen 21
*Sep 23 15:15:43.918: 00:40:96:ac:dd:05 processing avps[4]: attribute 80,
  vendorId 0, valueLen 16
```

Opmerking: Sommige lijnen in de debug-uitvoer zijn ingepakt door ruimtebeperkingen.

4. Controleer de logbestanden op de WLC om te controleren of de RADIUS-server de gebruikersreferenties ontvangt. Klik op **Monitor** om de logbestanden te controleren vanuit de WLC GUI. Klik in het linker zijmenu op **Statistieken** en klik vervolgens op **Radius server** in de lijst met opties. Dit is zeer belangrijk omdat in sommige gevallen de RADIUS-server nooit de gebruikersreferenties ontvangt als de RADIUS-serverconfiguratie op de WLC onjuist is. Dit is hoe de logbestanden op de WLC verschijnen als de RADIUS-parameters niet correct worden geconfigureerd:



U kunt een combinatie van de opdracht **Show WLAN** gebruiken om te herkennen welke van uw WLAN's RADIUS-serververificatie gebruiken. Vervolgens kunt u de opdracht **Show client summary** bekijken om te zien welke MAC-adressen (clients) met succes geauthentiseerd zijn op RADIUS WLAN's. U kunt dit ook correleren met uw Cisco Secure ACS-doorgegeven pogingen of mislukte pogingen.

Tips bij het oplossen van problemen

- Controleer op de controller dat de RADIUS-server **actief** is en niet **stand-by** of **uitgeschakeld**.
- Gebruik de opdracht **ping** om te controleren of de server Radius bereikbaar is vanaf de WLC.
- Controleer of de RADIUS-server is geselecteerd in het uitrolmenu van de WLAN (SSID).
- Als u WAP gebruikt, moet u de nieuwste Microsoft WAP-hotfix voor Windows XP SP2 installeren. U moet ook het stuurprogramma voor uw client uploaden naar de laatste.
- Als u bijvoorbeeld PEAP-certificaten met XP of SP2 doet, waar de kaarten worden beheerd door de Microsoft Wireless-0-applicatie, moet u de KB885453-patch van Microsoft krijgen. Als u Windows Zero Config/client gebruikt, schakelt u **Fast Reconconnect in**. U kunt dit doen als u kiest voor **eigenschappen van draadloze netwerkverbinding > Draadloze netwerken > Voorkeuren netwerken**. Kies vervolgens **SSID > Properties > Open > voorkomen > voorkomen > voorkomen > verificatie > EAP type > PEAP > Eigenschappen > Snel opnieuw aansluiten**. U kunt vervolgens de optie vinden om in- of uitschakelen in het venster.
- Als u Intel 2200- of 2915-kaarten hebt, zie dan de verklaringen op de website van Intel over bekende problemen met hun kaarten: [Intel® PRO/Wireless 2200BG netwerkverbinding](#) [Intel® PRO/Wireless 2915ABG netwerkverbinding](#) Download de huidige Intel chauffeurs om

problemen te voorkomen. U kunt Intel chauffeurs downloaden op

<http://downloadcenter.intel.com/>

- Als de agressieve failover optie in WLC is ingeschakeld, is de WLC te agressief om de AAA-server te markeren als `niet reageert`. Maar dit dient niet te worden gedaan omdat de AAA-server mogelijk niet alleen reageert op die bepaalde client, als je geen bericht teruggooit. Het kan een antwoord zijn op andere geldige cliënten met geldige certificaten. Maar de WLC kan de AAA-server nog steeds `niet markeren als niet reageert en niet functioneel`. Om dit te overwinnen, schakelt u de agressieve failover optie uit. Geef de **configuratie straal agressief-failover optie uit** van de controller GUI om dit uit te voeren. Als dit wordt uitgeschakeld, heeft de controller alleen een fout in de volgende AAA-server als er drie opeenvolgende klanten zijn die geen antwoord van de RADIUS-server ontvangen.

EAP-timers manipuleren

Tijdens de 802.1x-verificatie kan de gebruiker de `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE` zien: `MAX EAPOL-Key M1-terugzendingen bereikt voor mobiel xx:xx:xx:xx:xx` foutmelding.

Deze foutmeldingen geven aan dat de client niet tijdig heeft gereageerd op de controller tijdens de WAP-onderhandeling (802.1x). De controller stelt een timer in voor een respons tijdens belangrijke onderhandelingen. Meestal is dit bericht het gevolg van een probleem met de aanvrager. Zorg ervoor dat u de nieuwste versies van clientstuurprogramma's en firmware uitvoert. Op de WLC zijn er een paar MAP timers die je kunt manipuleren om te helpen met de authenticatie van klanten. Deze MAP-timers omvatten:

```
EAP-Identity-Request Timeout
EAP-Identity-Request Max Retries
EAP-Request Timeout (seconds)
EAP-Request Max Retries
EAPOL-Key Timeout
EAPOL-Key Max Retries
```

Voordat u deze waarden kunt manipuleren, moet u begrijpen wat ze doen, en hoe het veranderen ze van invloed zal zijn op het netwerk:

- **Time-outperiode voor MAP-identiteitsaanvraag:** Deze timer beïnvloedt hoe lang u wacht tussen MAP-identiteitsaanvragen. Standaard is dit één seconde (4.1 en lager) en 30 seconden (4.2 en hoger). De reden voor deze verandering was dat sommige klanten, handhelden, telefoons, scanners etc. het moeilijk hadden om snel genoeg te reageren. Apparaten als laptops vereisen meestal geen manipulatie van deze waarden. De beschikbare waarde is van 1 tot 120. Wat gebeurt er dan als deze eigenschap is ingesteld op een waarde van 30? Wanneer de client voor het eerst wordt aangesloten, verstuurt hij een EAPOL-start naar het netwerk en stuurt de WLC een EAP-pakket met een aanvraag voor de identiteit van de gebruiker of machine. Als de WLC de Identity Response niet ontvangt, wordt 30 seconden na de eerste identiteitsaanvraag een andere identiteitsaanvraag verzonden. Dit gebeurt bij de eerste verbinding, en wanneer de cliënt rondloopt. Wat gebeurt er als we deze timer verhogen? Als alles goed is, is er geen impact. Als er echter een probleem in het netwerk is (waaronder clientproblemen, AP-problemen of RF-problemen), kan dit vertragingen in de netwerkconnectiviteit veroorzaken. Als u de timer bijvoorbeeld instelt op de maximale waarde van 120 seconden, wacht de WLC 2 minuten tussen de identiteitsaanvragen. Als de klant

roaming is, en het antwoord niet door de WLC wordt ontvangen, dan hebben we minstens een uitval van twee minuten voor deze klant gecreëerd. Aanbevelingen voor deze timer is 5. Op dit moment is er geen reden om deze timer op zijn maximale waarde te plaatsen.

- **Max. antwoord MAP-aanvraag:**De waarde Max Retries is het aantal keer dat de WLC de Identity Aanvraag naar de client verstuurt voordat deze wordt verwijderd van de MSCB. Zodra de Max Retries zijn bereikt, stuurt de WLC een de-authenticatiekader naar de client, waardoor deze gedwongen wordt het MAP-proces opnieuw op te starten. De beschikbare waarde is 1 tot 20. Daarna zullen we dit nader bestuderen. The Max Retries werkt met de Time-out voor identiteit. Als u een Time-out voor uw identiteit hebt ingesteld op 120, en uw Max retourneert naar 20 hoe lang duurt dit 2400 (of $120 * 20$). Dit betekent dat het 40 minuten zou duren voordat de cliënt werd verwijderd en het MAP-proces opnieuw zou starten. Als u de Time-out voor identiteit instelt op 5, met een max. Retries-waarde van 12, dan duurt dit 60 (of $5 * 12$). In tegenstelling tot het vorige voorbeeld is er één minuut voordat de cliënt wordt verwijderd en moet worden gestart met EAP. Aanbevelingen voor de Max Retries zijn 12.
- **Time-outperiode van EAPOL:**Voor de EAPOL-Key Time-outwaarde is de standaard 1 seconde of 1000 milliseconden. Dit betekent dat wanneer de EAPOL-toetsen worden uitgewisseld tussen de AP en de client, de AP de toets zal verzenden en standaard tot 1 seconde zal wachten zodat de cliënt kan reageren. Na het wachten van de gedefinieerde tijdwaarde zal AP de toets opnieuw verzenden. U kunt de **configuratie geavanceerde eap eapol-key-timeout <tijd>opdracht** gebruiken om deze instelling te wijzigen. De beschikbare waarden in 6.0 zijn tussen 200 en 5000 milliseconden, terwijl de codes vóór 6.0 waarden tussen 1 en 5 seconden toestaan. Houd in gedachten dat als je een client hebt die niet reageert op een belangrijke poging, het uitbreiden van de timers een beetje meer tijd kan geven om te reageren. Dit kan echter ook de tijd verlengen die het voor de WLC/AP nodig heeft om de client opnieuw te certificeren, zodat het hele 802.1x-proces kan beginnen.
- **Max. reboeking EAPOL-Key:**Voor de EAPOL-Key Max Retries is de standaard 2. Dit betekent dat we de oorspronkelijke toets twee keer naar de client opnieuw proberen. Deze instelling kan gewijzigd worden met de **configuratie geavanceerde eap-eapol-key-opdracht**. De beschikbare waarden liggen tussen 0 en 4 herhalingen. Gebruik van de standaardwaarde voor de EAPOL-Key Time-out (d.w.z. 1 seconde) en de standaardwaarde voor de EAPOL-Key Retry (2) gaat het proces als volgt als een cliënt niet reageert op de initiële sleutel poging: De AP stuurt een belangrijke poging naar de cliënt. Het wacht een seconde om te antwoorden. Als er geen antwoord is, wordt het eerste EAPOL-Key Retry verstuurd. Het wacht een seconde om te antwoorden. Als er geen antwoord is, wordt de tweede EAPOL-Key Retry verstuurd. Als er nog steeds geen reactie van de cliënt is en de waarde van het opnieuw proberen is bereikt, dan wordt de cliënt gedeauthenticeerd. Nogmaals, zoals met de EAPOL-Key Time-out, zou een uitbreiding van de EAPOL-Key repowaarde in bepaalde omstandigheden nuttig kunnen zijn. Het instellen van het maximum kan echter opnieuw schadelijk zijn, aangezien het gedeauthenticeerde bericht langer geldig is.

[Het pakketbestand via een ACS-RADIUS-server voor probleemoplossing ophalen](#)

Als u ACS als de externe straal server gebruikt, kan deze sectie worden gebruikt om uw configuratie problemen op te lossen. The Packet.cab is een Zip-bestand dat alle benodigde bestanden bevat om een ACS-oplossing efficiënt te kunnen oplossen. U kunt de voorziening CSSsupport.exe gebruiken om het pakket.cab te maken, of u kunt de bestanden handmatig verzamelen.

Raadpleeg het gedeelte [Een pakket.cab File](#) van *het verkrijgen van versie en AAA bug Informatie voor Cisco Secure ACS voor Windows* voor meer informatie over het maken en extraheren van het pakketbestand uit WCS.

Gerelateerde informatie

- [WLAN-controller-failover voor lichtgewicht access points - Configuratievoorbeeld](#)
- [Software-upgrade van draadloze LAN-controller \(WLC\)](#)
- [Cisco draadloze LAN-controllers - handleiding](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)