

Een RADIUS-server en WLC configureren voor dynamische VLAN-toewijzing

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Dynamische VLAN-toewijzing met RADIUS-server](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuratie](#)

[Configuratiestappen](#)

[Configuratie van RADIUS-servers](#)

[ACS met Cisco Airesponderende VSA-kenmerken configureren voor dynamische VLAN-toewijzing](#)

[De Switch voor meerdere VLAN's configureren](#)

[WLC-configuratie](#)

[Configuratie van draadloos clienthulpprogramma](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document introduceert het concept dynamische VLAN-toewijzing. Het document beschrijft hoe u de draadloze LAN-controller (WLC) en een RADIUS-server kunt configureren om draadloze LAN-clients (WLAN) dynamisch aan een specifiek VLAN toe te wijzen.

Voorwaarden

Vereisten

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

- beschikken over basiskennis van de WLC en lichtgewicht access points (LAP's)
- beschikken over functionele kennis van de AAA-server
- Zorg voor een grondige kennis van draadloze netwerken en draadloze beveiligingsproblemen
- beschikken over basiskennis van lichtgewicht AP Protocol (LWAPP)

Gebruikte componenten

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

- Cisco 4400 WLC met firmware release 5.2
- Cisco 1130 Series LAP
- Cisco 802.11a/b/g draadloze clientadapter voor firmware release 4.4
- Cisco Aironet Desktop Utility (ADU) die versie 4.4 uitvoert
- Cisco Secure Access Control Server (ACS) met versie 4.1
- Cisco 2950 Series switch

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.](#)

Dynamische VLAN-toewijzing met RADIUS-server

In de meeste WLAN-systemen heeft elke WLAN-functie een statisch beleid dat van toepassing is op alle klanten die bij een Service Set Identifier (SSID) of WLAN in de controller-terminologie worden aangesloten. Hoewel krachtig, heeft deze methode beperkingen omdat het van cliënten vereist om met verschillende SSIDs te associëren om verschillend QoS en veiligheidsbeleid te erven.

De Cisco WLAN-oplossing ondersteunt echter identiteitsnetwerken. Dit staat het netwerk toe om één enkele SSID te adverteren, maar staat specifieke gebruikers toe om verschillend QoS of veiligheidsbeleid te erven gebaseerd op het gebruikersgeheugen.

Dynamische VLAN-toewijzing is één dergelijke functie die een draadloze gebruiker in een specifiek VLAN plaatst op basis van de referenties die door de gebruiker worden geleverd. Deze taak om gebruikers aan een specifiek VLAN toe te wijzen wordt behandeld door een RADIUS-verificatieserver, zoals Cisco Secure ACS. Dit kan bijvoorbeeld gebruikt worden om de draadloze host op hetzelfde VLAN te laten blijven terwijl het binnen een campus-netwerk beweegt.

Daarom, wanneer een client probeert te associëren met een LAP die geregistreerd is met een controller, geeft LAP de referenties van de gebruiker door aan de RADIUS-server voor validatie. Zodra de authenticatie succesvol is, passeert de RADIUS-server bepaalde eigenschappen van Internet Engineering Task Force (IETF) aan de gebruiker. Deze RADIUS-eigenschappen bepalen de VLAN-ID die aan de draadloze client moet worden toegewezen. De SSID (WLAN, in termen van WLC) van de client maakt niet uit omdat de gebruiker altijd aan deze vooraf bepaalde VLAN-ID wordt toegewezen.

De RADIUS-gebruikerseigenschappen die gebruikt worden voor de VLAN-ID-toewijzing zijn:

- IETF 64 (Tunnel type) - stel dit in op VLAN.
- IETF 65 (Middelgroot tunneltype) — Stel dit in op 802

- IETF 81 (Tunnel Private Group ID) - stel deze optie in op VLAN-id.

De VLAN ID is 12 bits en neemt een waarde tussen 1 en 4094, inclusief. Omdat de Tunnel-Private-Group-ID van type string is, zoals gedefinieerd in [RFC2868](#) voor gebruik met IEEE 802.1X, wordt de integerwaarde van VLAN ID gecodeerd als een string. Wanneer deze tunnelkenmerken worden verzonden, moet het veld Markering worden ingevuld.

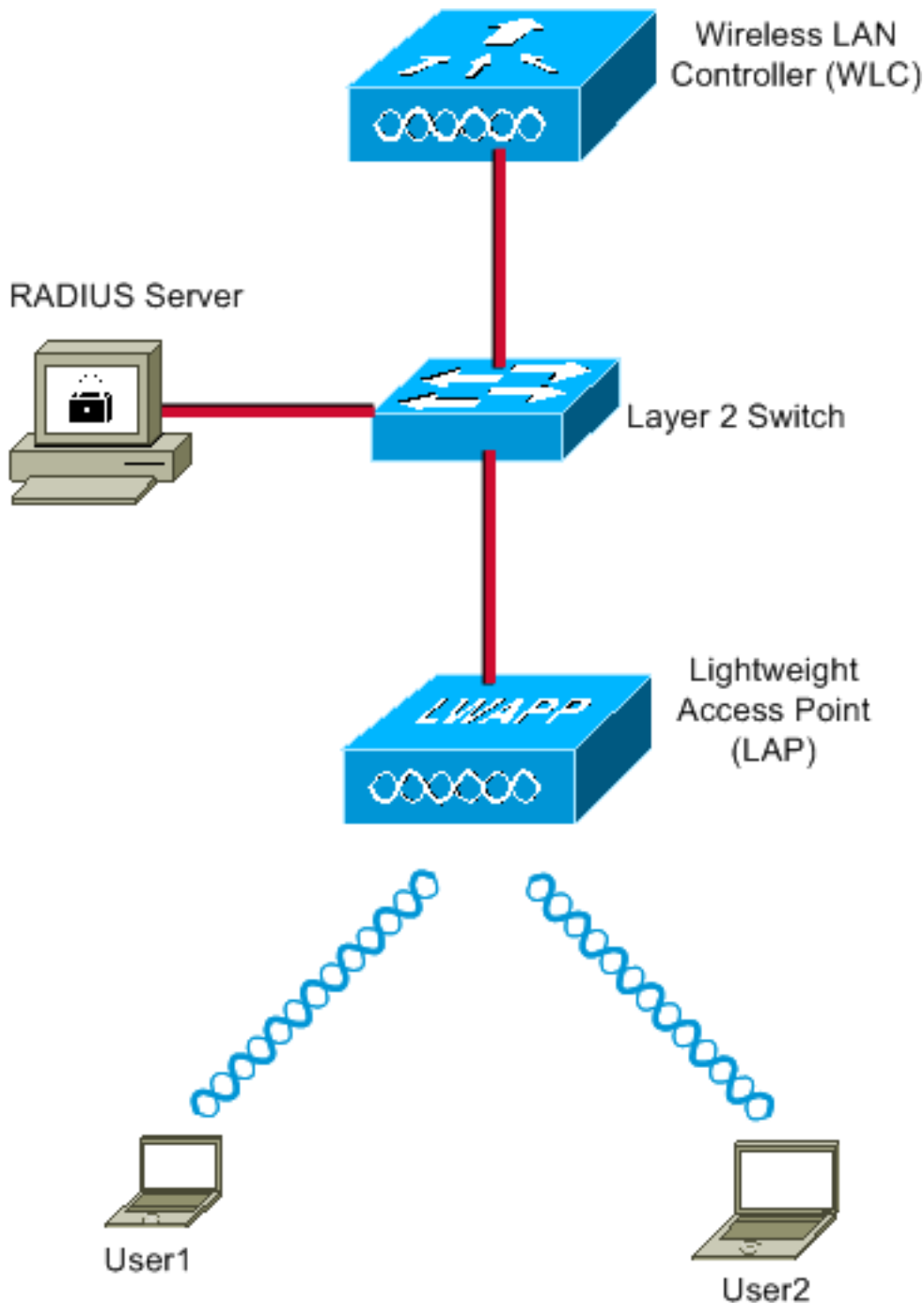
Zoals opgemerkt in [RFC2868](#), rubriek 3.1: **Het veld Markering is één octet lang en is bedoeld om een groepering van eigenschappen in hetzelfde pakket mogelijk te maken die betrekking hebben op dezelfde tunnel.** Geldige waarden voor dit veld zijn 0x01 tot 0x1F, inclusief. Als het veld Tag niet is gebruikt, moet het nul zijn (0x00). Raadpleeg [RFC 2868](#) voor meer informatie over alle RADIUS-kenmerken.

[Configureren](#)

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

[Netwerkdigram](#)

Het netwerk in dit document is als volgt opgebouwd:



Dit zijn de configuratiegegevens van de in dit schema gebruikte onderdelen:

- Het IP-adres van de ACS-server (RADIUS) is 172.16.1.1.
- Het Management Interface-adres van de WLC is 172.16.1.30.
- Het AP-Manager interfaceadres van de WLC is 172.16.1.31.
- Het DHCP-serveradres 172.16.1.1 wordt gebruikt om IP-adressen aan de LWAPP toe te wijzen. **De interne DHCP-server op de controller wordt gebruikt om het IP-adres aan draadloze klanten toe te wijzen.**
- VLAN10 en VLAN11 worden gebruikt door deze configuratie. Gebruiker1 wordt ingesteld om in VLAN10 te worden geplaatst en user2 wordt geconfigureerd om in VLAN11 door de RADIUS-server te worden geplaatst. **N.B.:** Dit document toont alleen alle configuratieinformatie met betrekking tot gebruiker1. Vul de in dit document beschreven procedure in voor de gebruiker2.
- In dit document wordt 802.1x met LEAP als veiligheidsmechanisme gebruikt. **Opmerking:** Cisco raadt u aan geavanceerde authenticatiemethoden, zoals EAP-FAST en EAP-TLS-

verificatie, te gebruiken om de WLAN-verificatie te beveiligen. In dit document wordt alleen LEAP gebruikt voor de eenvoud.

[Configuratie](#)

Vóór de configuratie wordt er in dit document van uitgegaan dat de LAP al bij de WLC is geregistreerd. Raadpleeg de [lijst met draadloze LAN-controllers en lichtgewicht access point voor basisconfiguratie](#) voor meer informatie. Raadpleeg de [LAP-registratie \(Lichtgewicht AP\) bij een draadloze LAN-controller \(WLC\)](#) voor informatie over de registratieprocedure.

[Configuratiestappen](#)

Deze configuratie is in drie categorieën verdeeld:

1. [Configuratie van RADIUS-servers](#)
2. [De Switch voor meerdere VLAN's configureren](#)
3. [WLC-configuratie](#)
4. [Configuratie van draadloos clienthulpprogramma](#)

[Configuratie van RADIUS-servers](#)

Voor deze configuratie zijn de volgende stappen vereist:

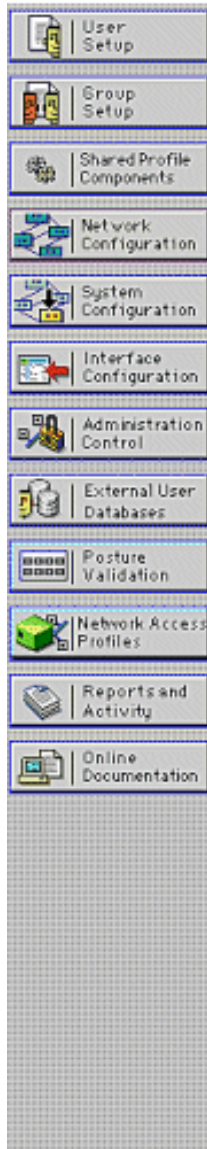
- [De WLC configureren als een AAA-client op de RADIUS-server](#)
- [Configureer de gebruikers en de RADIUS \(IETF\) kenmerken die worden gebruikt voor dynamische VLAN-toewijzing op de RADIUS-server](#)

[AAA-client voor de WLC configureren op de RADIUS-server](#)

Deze procedure legt uit hoe de WLC als een AAA-client op de RADIUS-server moet worden toegevoegd, zodat de WLC de gebruikersreferenties aan de RADIUS-server kan doorgeven.

Voer de volgende stappen uit:

1. Klik vanuit de ACS GUI op **Netwerkconfiguratie**.
2. Klik het gedeelte **Ingang toevoegen** onder het veld AAA-clients.
3. Voer het AAA client-IP-adres en -toets in. Het IP-adres moet het IP-adres van de beheerinterface van de WLC zijn. Zorg ervoor dat de toets die u invoert, dezelfde is als de toets die in het WLC onder het Security venster is ingesteld. Dit is de geheime sleutel die wordt gebruikt voor communicatie tussen de AAA client (WLC) en de RADIUS-server.
4. Kies **RADIUS (Cisco Aironet)** van het veld Verificeren met het verificatietype.



Add AAA Client

AAA Client Hostname	<input type="text" value="WLC4400"/>
AAA Client IP Address	<input type="text" value="172.16.1.30"/>
Shared Secret	<input type="text" value="cisco"/>

RADIUS Key Wrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format ASCII Hexadecimal

Authenticate Using

Single Connect TACACS+ AAA Client (Record stop in accounting on failure)

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

[Configureer de gebruikers en de RADIUS \(IETF\) kenmerken die worden gebruikt voor dynamische VLAN-toewijzing op de RADIUS-server](#)

Deze procedure legt uit hoe u de gebruikers in de RADIUS-server en de RADIUS-kenmerken (IETF) kunt configureren die worden gebruikt om VLAN-ID's aan deze gebruikers toe te wijzen.

Voer de volgende stappen uit:

1. Klik in de ACS GUI op **Gebruikersinstelling**.
2. Typ in het venster Gebruikersinstelling een gebruikersnaam in het veld Gebruiker en klik op **Toevoegen/Bewerken**.



User Setup

Select

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

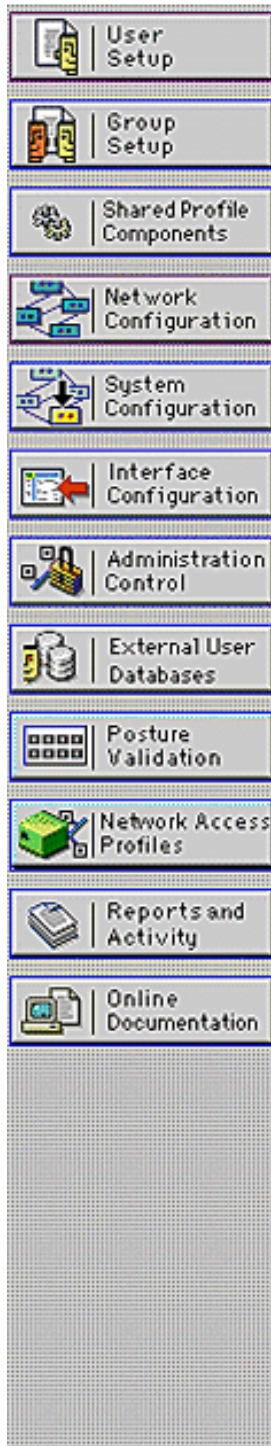
User:

List users beginning with letter/number:

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#)
[N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)
[0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

[Back to Help](#)

3. Voer in de pagina Bewerken de gewenste gebruikersinformatie in zoals hieronder wordt weergegeven:



User: User1

Account Disabled

Supplementary User Info

Real Name

Description

User Setup

Password Authentication:

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password

Confirm Password

Separate (CHAP/MS-CHAP/ARAP)

Password

Confirm Password

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

In dit diagram, merk op dat het wachtwoord dat u onder de sectie van de Instellen van de Gebruiker hebt opgegeven, hetzelfde zou moeten zijn als het wachtwoord dat aan de kant van de client tijdens de gebruikersverificatie is verstrekt.

4. Scrollt door de pagina Bewerken en vindt het veld **RADIUS-kenmerken van IETF**.
5. In het veld RADIUS-kenmerken van IETF controleert u de vinkjes naast de drie eigenschappen van de Tunnel en vervolgens configureren u de waarden van de kenmerken zoals hieronder wordt weergegeven:



User Setup

- User Setup
- Group Setup
- Shared Profile Components
- Network Configuration
- System Configuration
- Interface Configuration
- Administration Control
- External User Databases
- Posture Validation
- Network Access Profiles
- Reports and Activity
- Online Documentation

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL: VPN_Access

IETF RADIUS Attributes

[064] Tunnel-Type

Tag 1 Value VLAN

Tag 2 Value

[065] Tunnel-Medium-Type

Tag 1 Value 802

Tag 2 Value

[081] Tunnel-Private-Group-ID

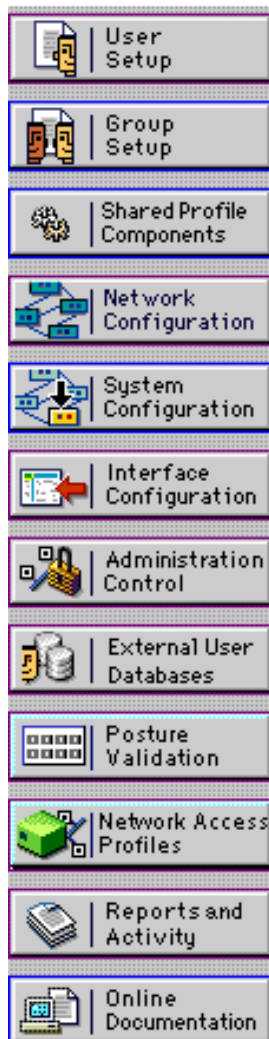
Tag 1 Value 10

Tag 2 Value

Opmerking: In de eerste configuratie van de ACS-server worden de RADIUS-kenmerken van IETF mogelijk niet weergegeven. Kies **Interface Configuration > RADIUS (IETF)** om de IETF-eigenschappen in het venster voor de gebruikersconfiguratie in te schakelen. Controleer vervolgens de vinkjes voor de eigenschappen **64**, **65** en **81** in de User and Group kolommen.



Interface Configuration

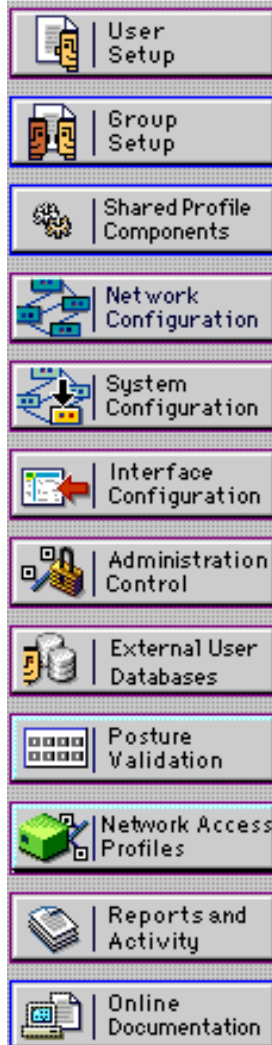


- [029] Termination-Action
- [033] Proxy-State
- [034] Login-LAT-Service
- [035] Login-LAT-Node
- [036] Login-LAT-Group
- [037] Framed-AppleTalk-Link
- [038] Framed-AppleTalk-Network
- [039] Framed-AppleTalk-Zone
- [062] Port-Limit
- [063] Login-LAT-Port
- [064] Tunnel-Type
- [065] Tunnel-Medium-Type
- [066] Tunnel-Client-Endpoint
- [067] Tunnel-Server-Endpoint
- [069] Tunnel-Password
- [071] ARAP-Features
- [072] ARAP-Zone-Access
- [078] Configuration-Token
- [081] Tunnel-Private-Group-ID
- [082] Tunnel-Assignment-ID
- [083] Tunnel-Preference
- [085] Acct-Interim-Interval
- [090] Tunnel-Client-Auth-ID
- [091] Tunnel-Server-Auth-ID

Opmerking: om de RADIUS-server dynamisch aan een specifiek VLAN toe te wijzen, moet de VLAN-ID die onder het veld IETF 81 (Tunnel-Private-Group-ID) van de RADIUS-server is geconfigureerd, op de WLC bestaan. Controleer de optie Per gebruiker TACACS+/RADIUS-kenmerken onder Interface Configuration > Advanced Opties om de RADIUS-server voor elke gebruikersconfiguratie in te schakelen. Zorg er ook voor, omdat LEAP wordt gebruikt als het verificatieprotocol, dat LEAP is ingeschakeld in het venster System Configuration van de RADIUS-server zoals hier wordt getoond:



System Configuration



Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

EAP-FAST

[EAP-FAST Configuration](#)

EAP-TLS

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

LEAP

Allow LEAP (For Aironet only)

EAP-MD5

Allow EAP-MD5

AP EAP request timeout (seconds):

[ACS met Cisco Airesponderende VSA-kenmerken configureren voor dynamische VLAN-toewijzing](#)

In de meest recente ACS-versies kunt u ook de eigenschap Cisco AIR [VSA (Vendor-Specific)] configureren om een succesvol geauthentiseerde gebruiker met een VLAN-interfacenaam (niet de VLAN ID) toe te wijzen zoals per de gebruikersconfiguratie op de ACS. Voer de stappen in deze sectie uit om dit te bereiken.

Opmerking: In deze sectie wordt de ACS 4.1-versie gebruikt om de Cisco Airespace VSA-eigenschap te configureren.

[Configuratie van de ACS-groep met de optie Cisco Airesponderende VSA-kenmerken](#)

Voer de volgende stappen uit:

1. Klik vanuit de ACS 4.1 GUI op **Interface Configuration** vanuit de navigatiebalk. Selecteer vervolgens **RADIUS (Cisco Airespace)** van de pagina Interface Configuration om de optie Cisco Airespace-kenmerk te configureren.
2. Controleer vanuit het RADIUS-venster (Cisco Airespace) het selectieteken van de gebruikersgroep (indien nodig het vakje Group check) naast **Aire-Interface-Name** om dit op de pagina met Gebruikersbewerking weer te geven. Klik vervolgens op **Inzenden**.

CISCO SYSTEMS

Interface Configuration

Edit

RADIUS (Cisco Airespace)

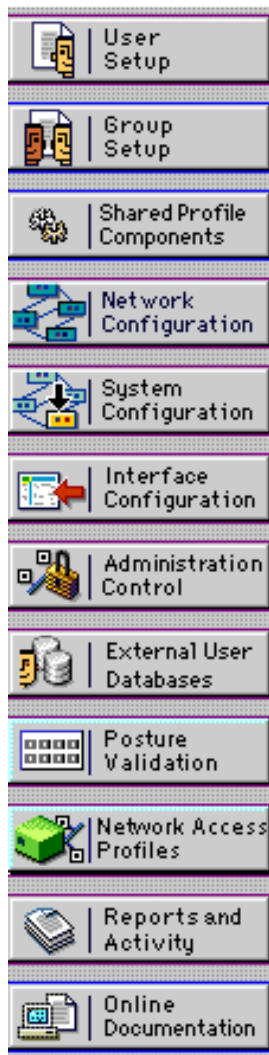
User	Group
<input type="checkbox"/>	<input type="checkbox"/> [026/14179/002] Aire-QoS-Level
<input type="checkbox"/>	<input type="checkbox"/> [026/14179/003] Aire-DSCP
<input type="checkbox"/>	<input type="checkbox"/> [026/14179/004] Aire-802.1P-Tag
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> [026/14179/005] Aire-Interface-Name
<input type="checkbox"/>	<input type="checkbox"/> [026/14179/006] Aire-Acl-Name

[? Back to Help](#)

3. Ga naar de pagina Bewerken van gebruiker1.
4. Klik op de pagina Bewerken door gebruiker op de sectie **RADIUS-kenmerken** van **Cisco Airespace**. Controleer het aankruisvakje naast het kenmerk **Aire-Interface-Name** en specificeer de naam van de dynamische interface die moet worden toegewezen bij succesvolle gebruikersverificatie. Dit voorbeeld wijst de gebruiker aan om **VLAN te beheren**.



User Setup



Date exceeds:

May 24 2009

Failed attempts exceed:

5

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

Downloadable ACLs

Assign IP ACL:

VPN_Access

Cisco Airespace RADIUS Attributes

[14179\005] Aire-Interface-Name

admin

5. Klik op **Inzenden**.

[De Switch voor meerdere VLAN's configureren](#)

Om meerdere VLAN's door de switch te laten lopen, moet u deze opdrachten uitvoeren om de switch poort te configureren die op de controller is aangesloten:

1. Switch (configuratie-als)#**Switch Mode**
2. Switch (-als)#**switchport boomstam insluitingpunt1q**

Opmerking: Standaard staan de meeste switches alle VLAN's toe die op die switch via de boomstampoort zijn gemaakt.

Deze opdrachten verschillen van de switch Catalyst 3000 (CatOS).

Als een bekabeld netwerk op de switch is aangesloten, kan deze configuratie worden toegepast op de switch die op het bekabelde netwerk aangesloten is. Dit maakt de communicatie tussen dezelfde VLAN's in het bekabelde en draadloze netwerk mogelijk.

N.B.: Dit document bespreekt de communicatie tussen VLAN's niet. Dit valt buiten het toepassingsgebied van dit document. U moet begrijpen dat voor de routing tussen VLAN's, een

Layer 3-switch of een externe router met goed VLAN en trunking-configuraties nodig zijn. Er zijn verschillende documenten die de routeringsconfiguratie tussen VLAN's verklaren.

[WLC-configuratie](#)

Voor deze configuratie zijn de volgende stappen vereist:

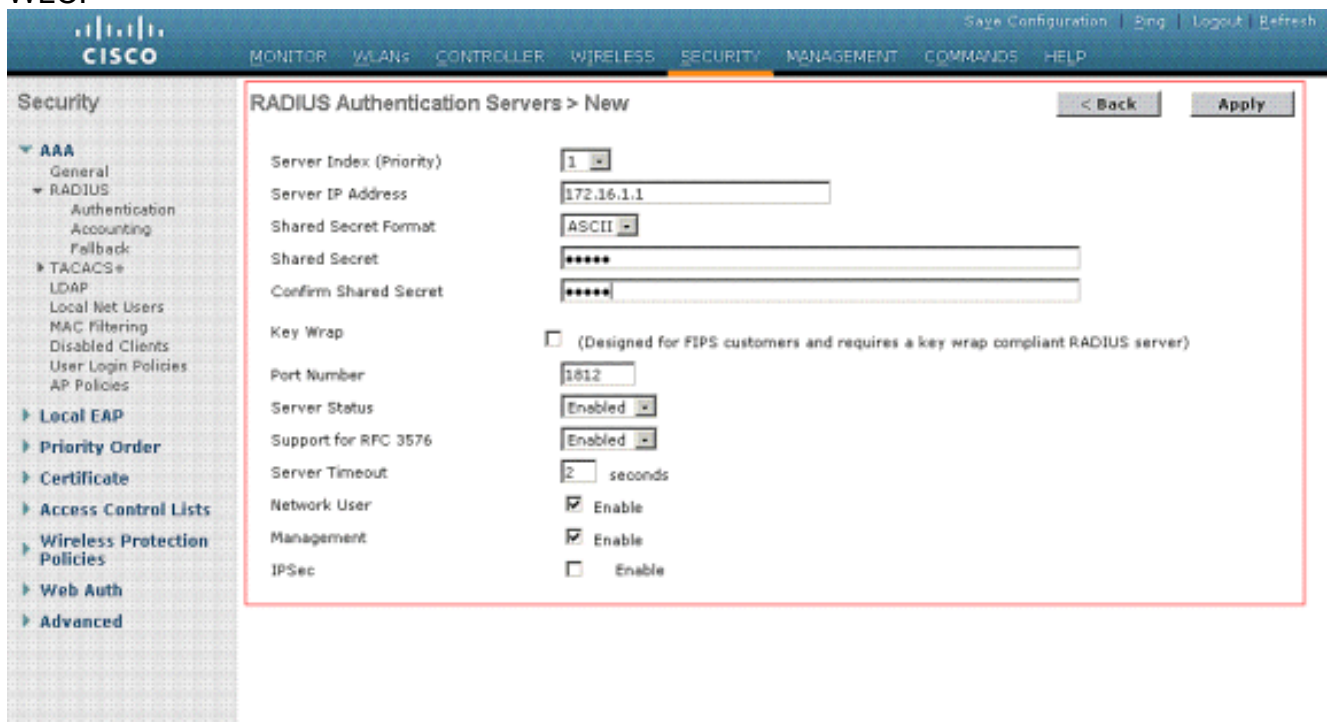
- [Het configureren van de WLC met de details van de verificatieserver](#)
- [Configuratie van de Dynamische interfaces \(VLAN's\)](#)
- [De WLAN's \(SSID's\) configureren](#)

[Het configureren van de WLC met de details van de verificatieserver](#)

Het is nodig om de WLC te configureren zodat het kan communiceren met de RADIUS-server om de clients te authenticeren, en ook voor andere transacties.

Voer de volgende stappen uit:

1. Klik vanuit de controller GUI op **Security**.
2. Voer het IP-adres in van de RADIUS-server en de gedeelde beveiligingstoets die wordt gebruikt tussen de RADIUS-server en de WLC. Deze gedeelde beveiligingstoets moet gelijk zijn aan de toets die is ingesteld in de RADIUS-server onder Netwerkconfiguratie > AAA-clients > Toevoegen. Hier is een voorbeeldvenster van de WLC:



The screenshot shows the Cisco WLC GUI with the 'Security' tab selected. The left sidebar shows a tree view with 'AAA' expanded to 'RADIUS'. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following configuration fields:

Server Index (Priority)	1
Server IP Address	172.16.1.1
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

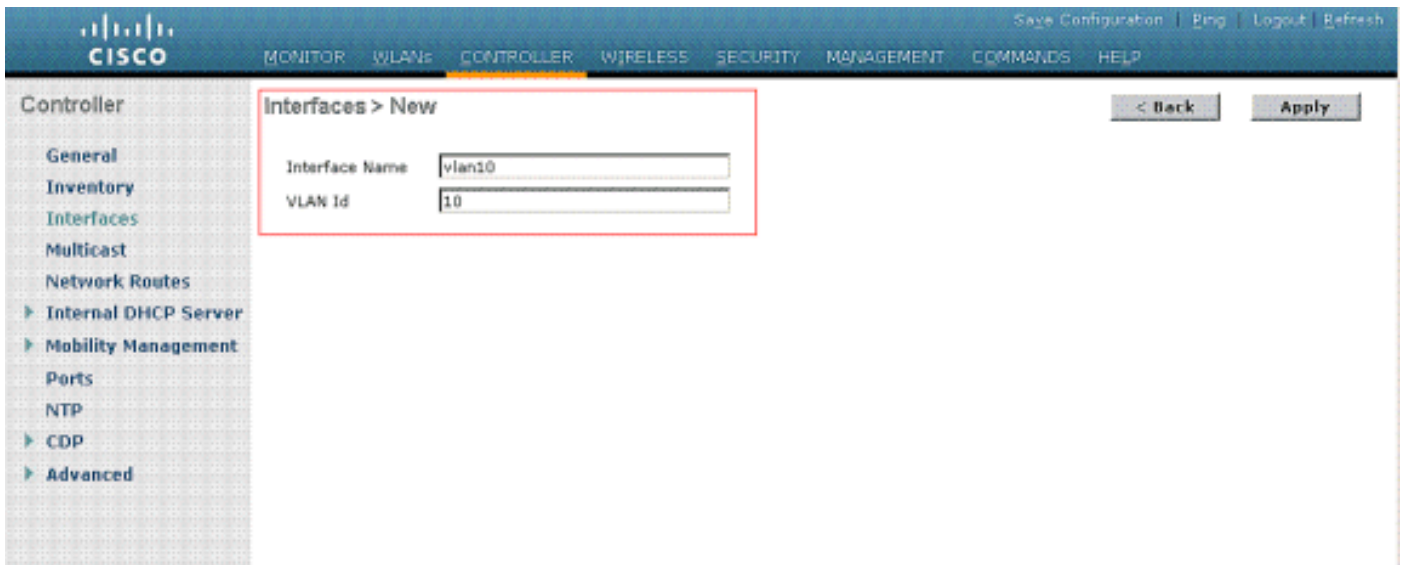
[Configuratie van de Dynamische interfaces \(VLAN's\)](#)

Deze procedure legt uit hoe u dynamische interfaces op de WLC kunt configureren. Zoals eerder in dit document wordt uitgelegd, moet de VLAN-ID die onder de eigenschap Tunnel-Private-Group ID van de RADIUS-server is gespecificeerd, ook in de WLC voorkomen.

In het voorbeeld, wordt user1 gespecificeerd met **Tunnel-Private-Group ID van 10 (VLAN=10)** op

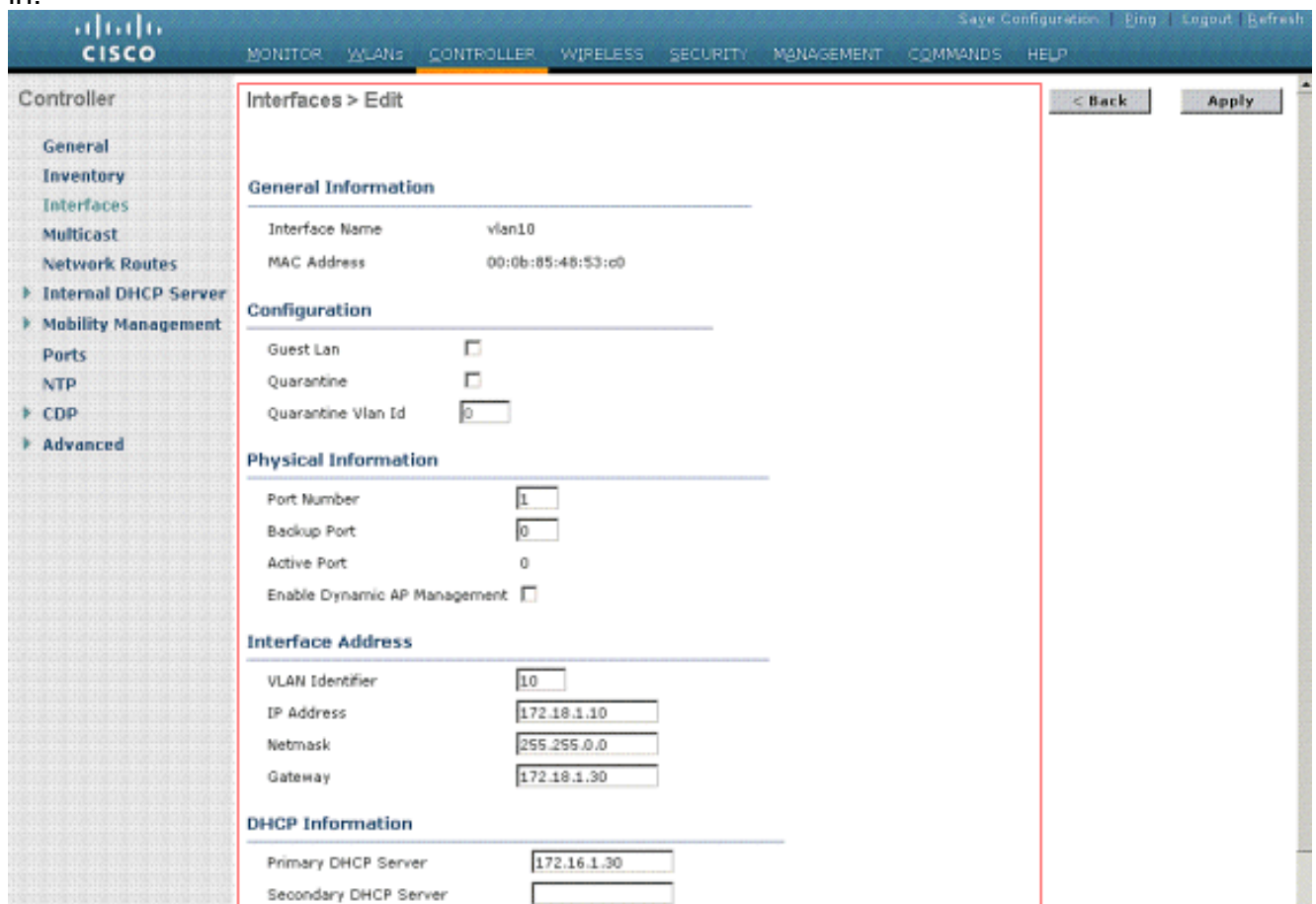
de RADIUS-server. Zie het gedeelte [RADIUS-kenmerken](#) van [IETF](#) in het venster User1 User Setup.

U kunt dezelfde dynamische interface (VLAN=10) zien die in WLC in dit voorbeeld is geconfigureerd. Vanuit de controller GUI, onder het venster Controller > Interfaces, wordt de dynamische interface geconfigureerd.



The screenshot shows the Cisco WLC GUI with the 'Controller' menu on the left. The main content area is titled 'Interfaces > New'. It contains two input fields: 'Interface Name' with the value 'vlan10' and 'VLAN Id' with the value '10'. There are '< Back' and 'Apply' buttons at the top right of the configuration area.

1. Klik op **Toepassen** in dit venster. Dit brengt u naar het venster Bewerken van deze dynamische interface (VLAN 10 hier).
2. Voer het IP-adres en de standaardgateway van deze dynamische interface in.



The screenshot shows the Cisco WLC GUI with the 'Controller' menu on the left. The main content area is titled 'Interfaces > Edit'. It is divided into several sections:

- General Information:** Interface Name: vlan10, MAC Address: 00:0b:85:48:53:c0
- Configuration:** Guest Lan: , Quarantine: , Quarantine Vlan Id:
- Physical Information:** Port Number: , Backup Port: , Active Port: 0, Enable Dynamic AP Management:
- Interface Address:** VLAN Identifier: , IP Address: , Netmask: , Gateway:
- DHCP Information:** Primary DHCP Server: , Secondary DHCP Server:

There are '< Back' and 'Apply' buttons at the top right of the configuration area.

N.B.: Omdat dit document een interne DHCP-server op de controller gebruikt, wijst het primaire DHCP-serverveld van dit venster op de Management-interface van de WLC zelf. U

kunt ook een externe DHCP-server, een router of de RADIUS-server zelf gebruiken als een DHCP-server naar de draadloze clients. In dergelijke gevallen wijst het primaire DHCP-serverveld naar het IP-adres van het apparaat dat als DHCP-server wordt gebruikt. Raadpleeg de documentatie op de DHCP-server voor meer informatie.

3. Klik op **Apply** (Toepassen). U bent nu ingesteld met een dynamische interface in uw WLC. Op dezelfde manier kunt u verschillende dynamische interfaces in uw WLC configureren. Vergeet echter niet dat dezelfde VLAN-id ook in de RADIUS-server moet voorkomen zodat dat VLAN aan de client wordt toegewezen.

[De WLAN's \(SSID's\) configureren](#)

Deze procedure legt uit hoe de WLAN's in de WLC moeten worden configureren.

Voer de volgende stappen uit:

1. Kies vanuit de controller GUI **WLAN's > New** om een nieuw WLAN te maken. Het venster New WLAN's wordt weergegeven.
2. Voer de WLAN-id en WLAN-informatie in. U kunt een naam invoeren om WLAN SSID te zijn. Dit voorbeeld gebruikt VLAN10 als WLAN SSID.

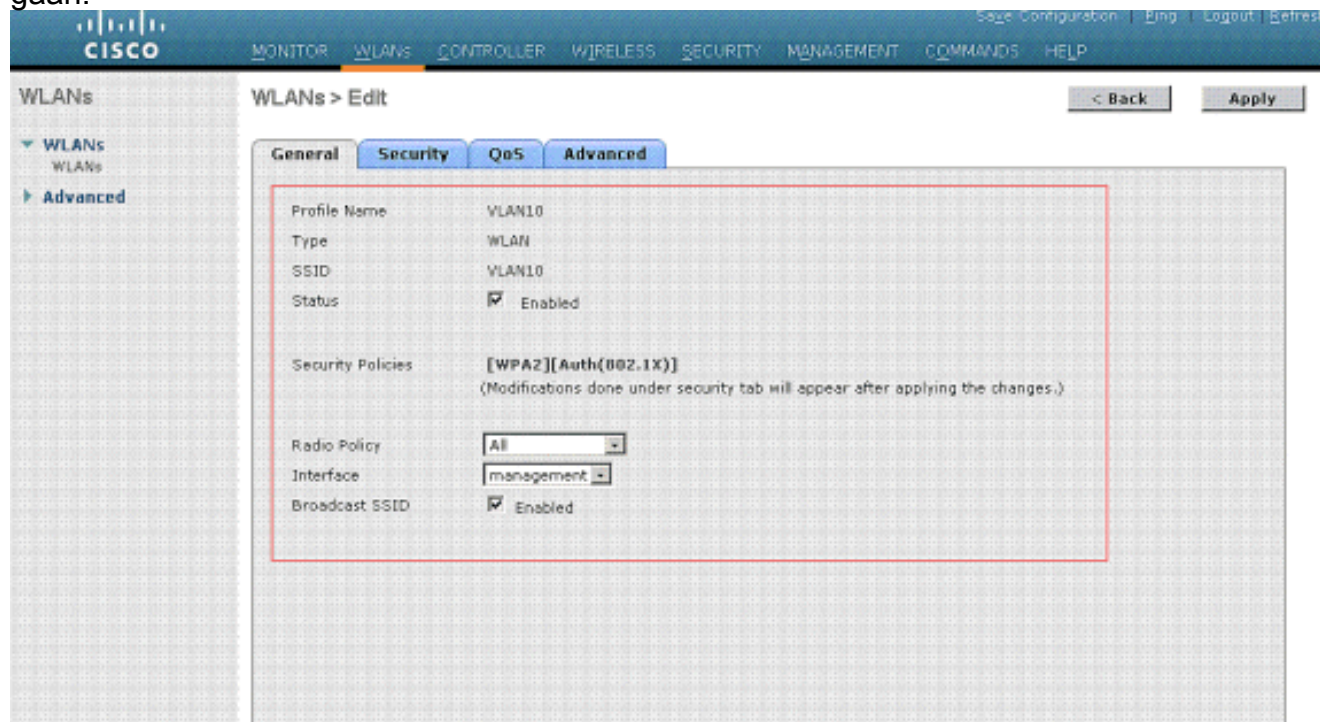


The screenshot shows the Cisco WLC GUI for creating a new WLAN. The page title is 'WLANs > New'. The left sidebar shows 'WLANs' and 'Advanced'. The main content area has a red box around the following fields:

Type	WLAN
Profile Name	VLAN10
SSID	VLAN10
ID	3

Buttons for '< Back' and 'Apply' are visible on the right.

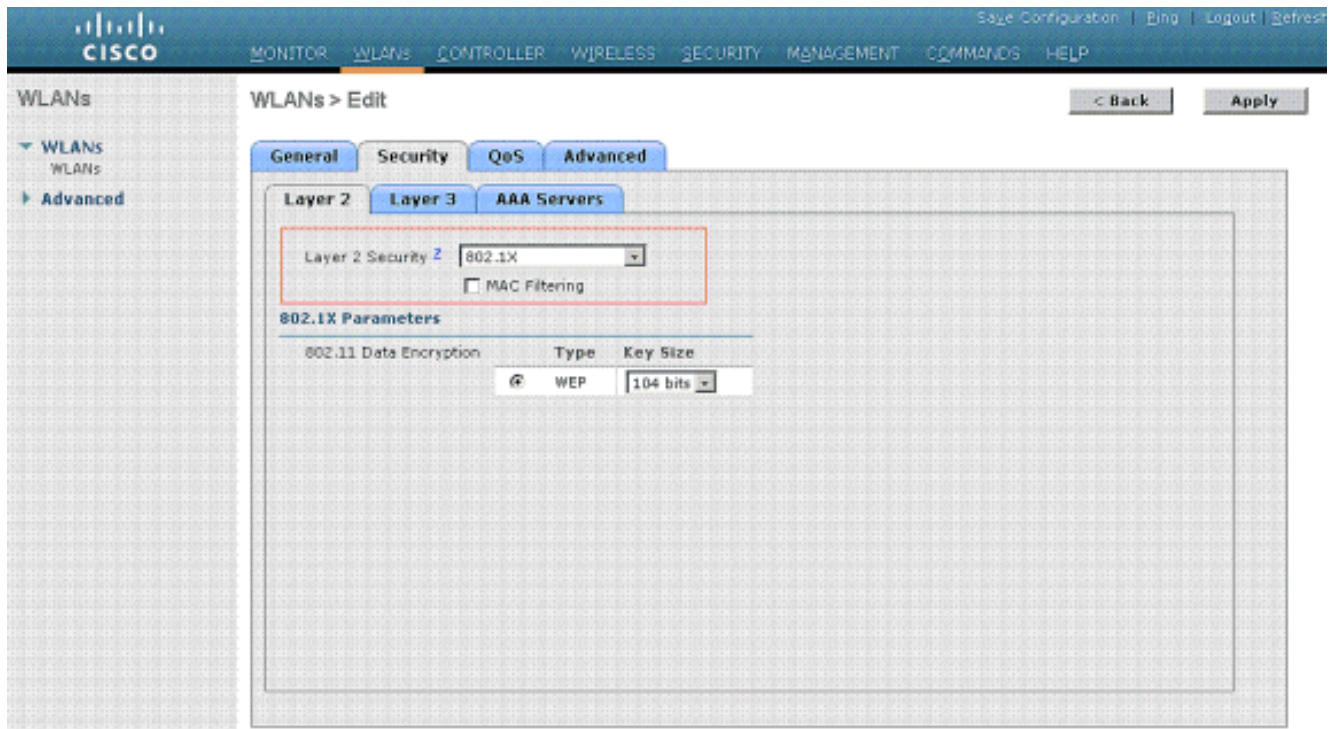
3. Klik op **Toepassen** om naar het venster Bewerken van de WLAN SSID10 te gaan.



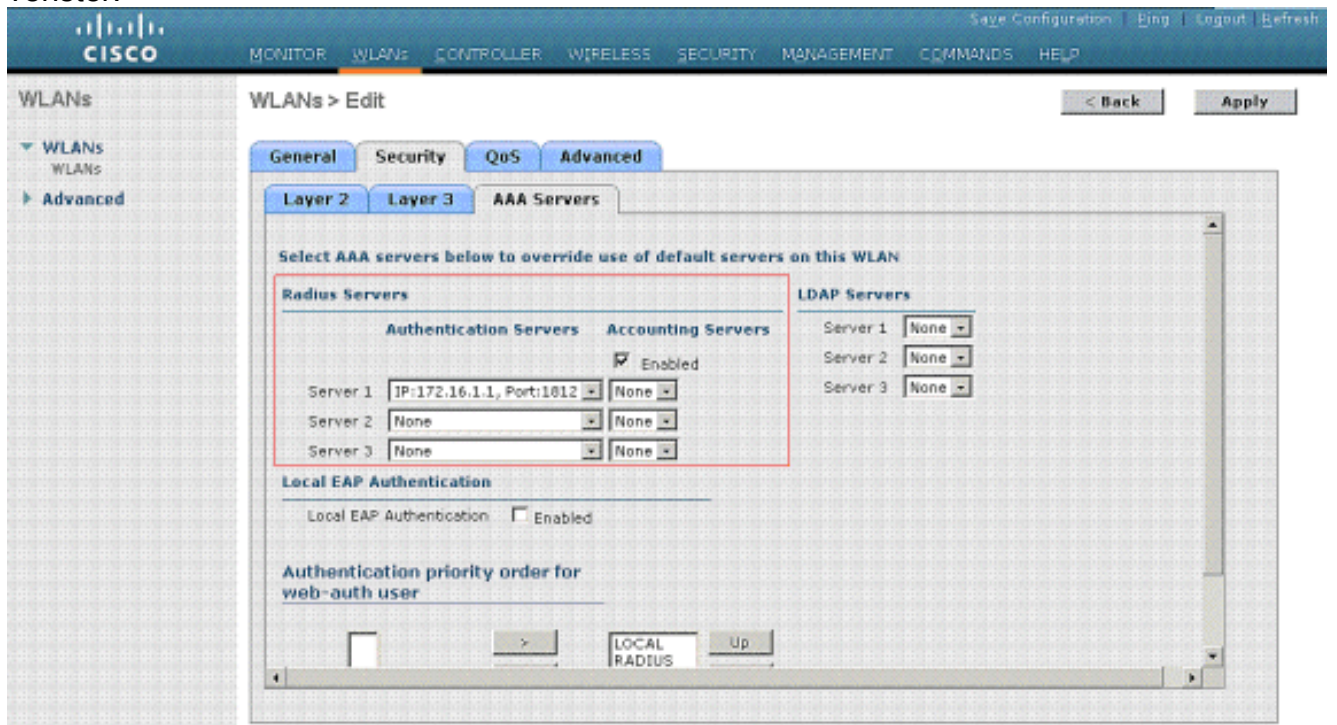
The screenshot shows the Cisco WLC GUI for editing a WLAN. The page title is 'WLANs > Edit'. The left sidebar shows 'WLANs' and 'Advanced'. The main content area has a red box around the following fields:

Profile Name	VLAN10
Type	WLAN
SSID	VLAN10
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(002.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface	management
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

Buttons for '< Back' and 'Apply' are visible on the right.



Normaal gesproken wordt elke WLAN-controller in kaart gebracht aan een specifiek VLAN (SSID), zodat een bepaalde gebruiker die bij die WLAN hoort, in het specifieke VLAN-kaart wordt gezet. Deze afbeelding wordt normaal gesproken uitgevoerd onder het veld Interfacenaam van het WLAN-venster.

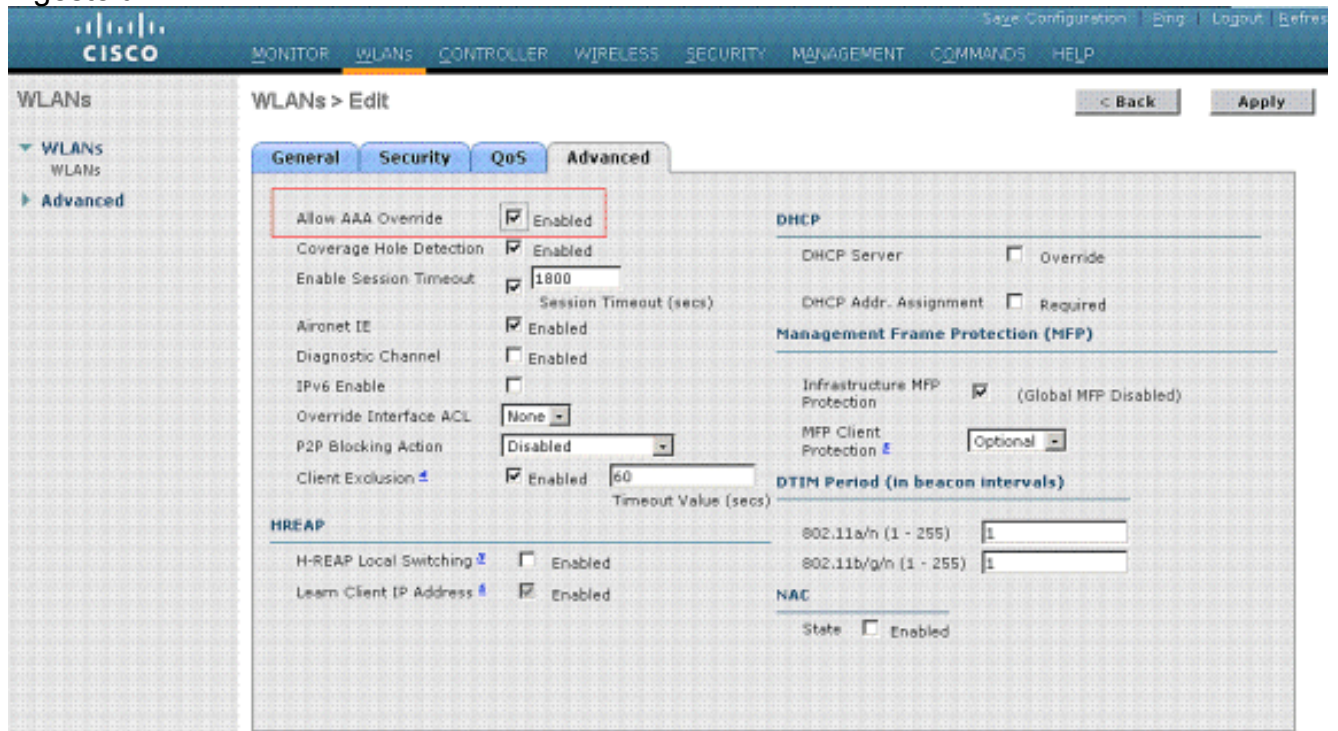


In het voorbeeld dat wordt gegeven, is het de taak van de RADIUS-server om een draadloze client aan een specifiek VLAN toe te wijzen bij succesvolle verificatie. De WLAN's hoeven niet in kaart te worden gebracht aan een specifieke dynamische interface in de WLC. Of, zelfs al wordt de WLAN-naar-dynamische interfacekaart op de WLC uitgevoerd, heeft de RADIUS-server deze mapping en wijst de gebruiker die door dat WLAN wordt ontvangen toe aan het VLAN dat wordt gespecificeerd onder het veld **Tunnel-Group-Private-ID** in de RADIUS-server.

4. Controleer het aanvinkvakje **AAA** negeren om de WLC-configuraties te omzeilen met de

RADIUS-server.

- Schakel de optie AAA-override in in de controller voor elke WLAN (SSID) ingesteld.



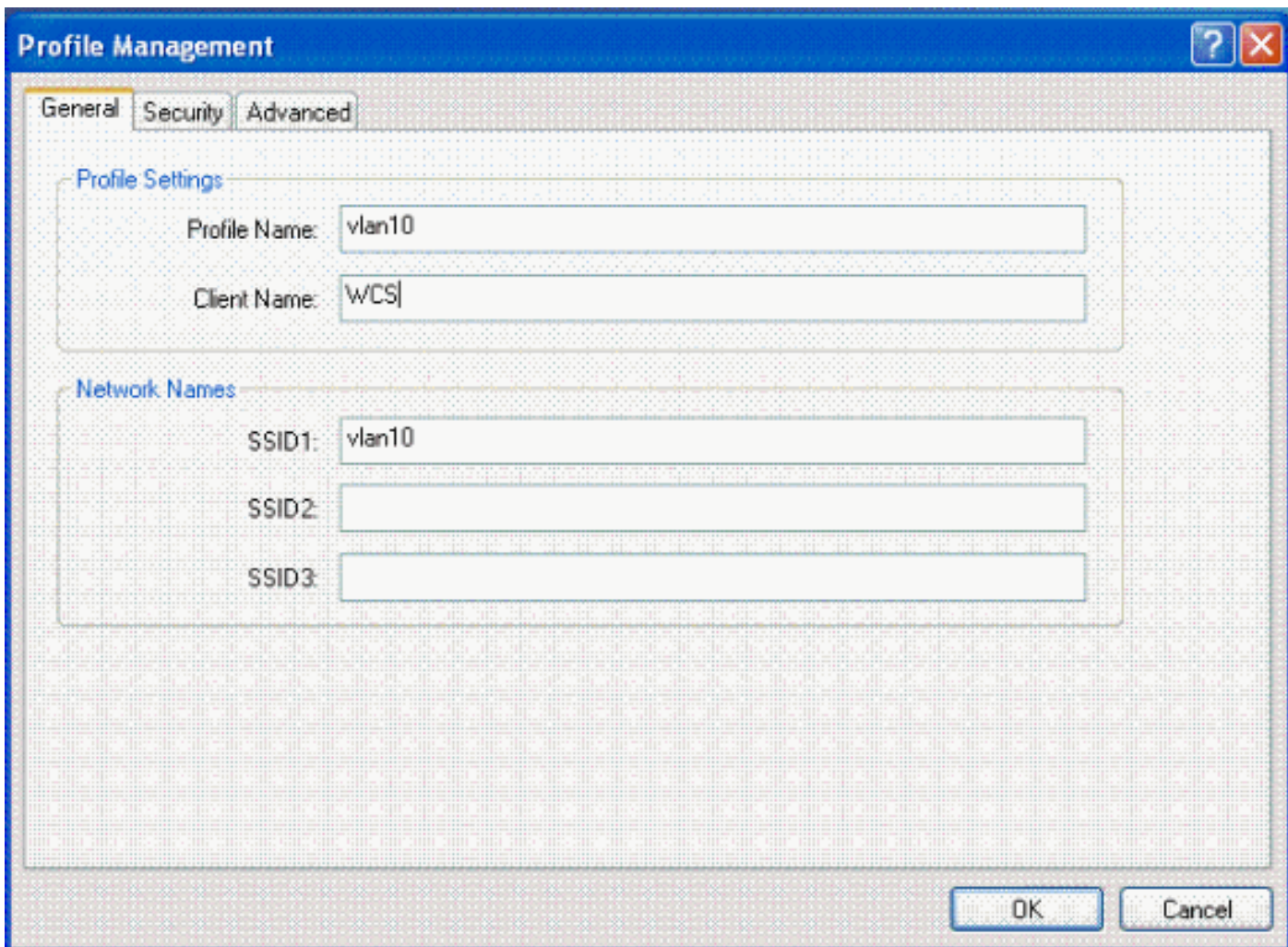
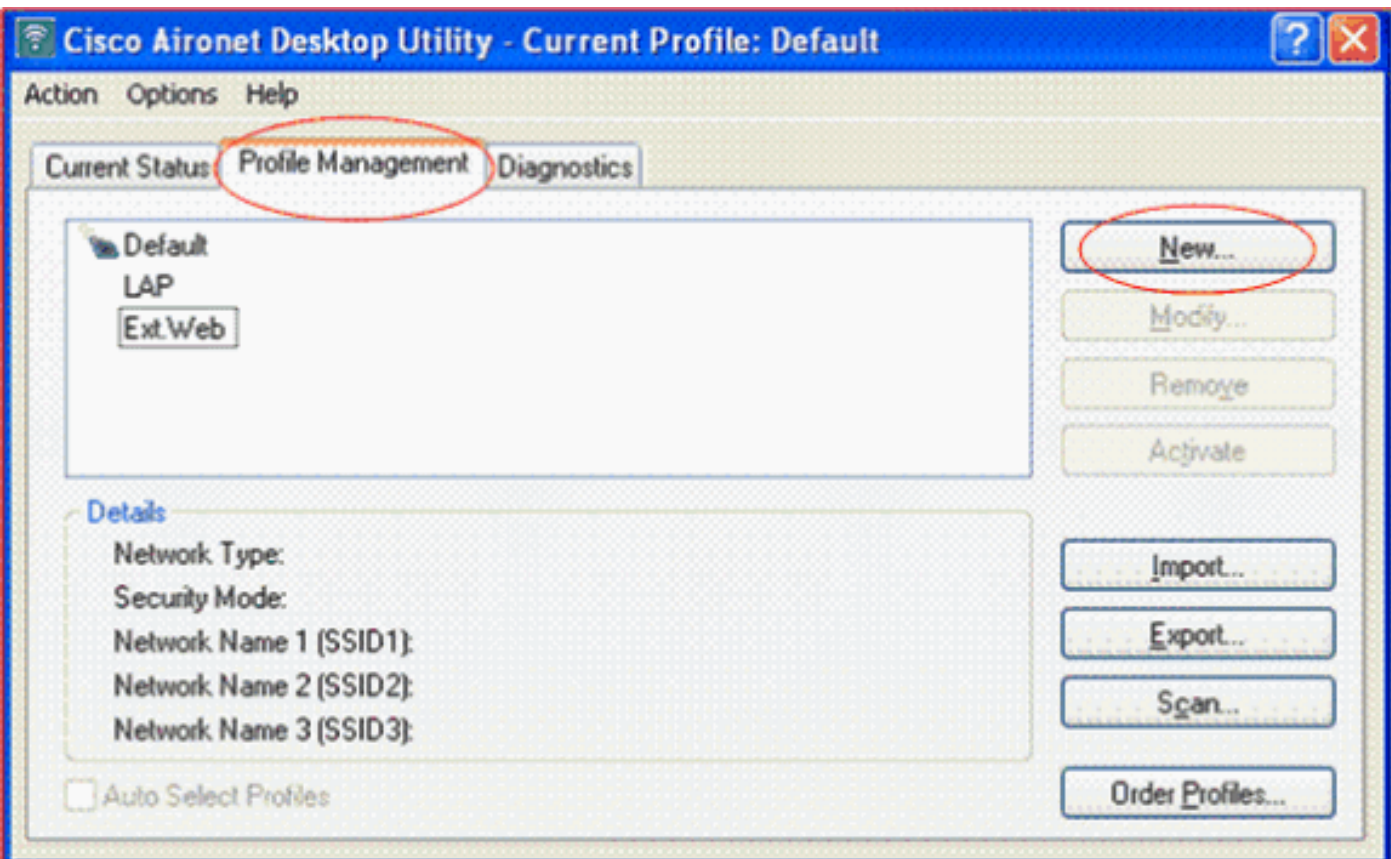
Wanneer AAA Override is geactiveerd en een client heeft AAA en controller WLAN-verificatieparameters die conflict opleveren, wordt client-verificatie uitgevoerd door de AAA (RADIUS) server. Als deel van deze authenticatie beweegt het besturingssysteem klanten naar een VLAN dat door de AAA server wordt getourneerd. Dit wordt vooraf gedefinieerd in de configuratie van de controller-interface. Als bijvoorbeeld de bedrijfsWLAN's voornamelijk een beheerinterface gebruiken die aan VLAN 2 is toegewezen, en als de AAA-override een redirect naar VLAN 100 teruggeeft, wijst het besturingssysteem alle clienttransmissie naar VLAN 100 opnieuw uit, zelfs als de fysieke poort waaraan VLAN 100 is toegewezen. Wanneer AAA Override is uitgeschakeld, blijft alle client-verificatie standaard voldoen aan de instellingen van de controller-authenticatieparameter en wordt verificatie alleen uitgevoerd door de AAA-server als de controller WLAN geen client-specifieke verificatieparameters bevat.

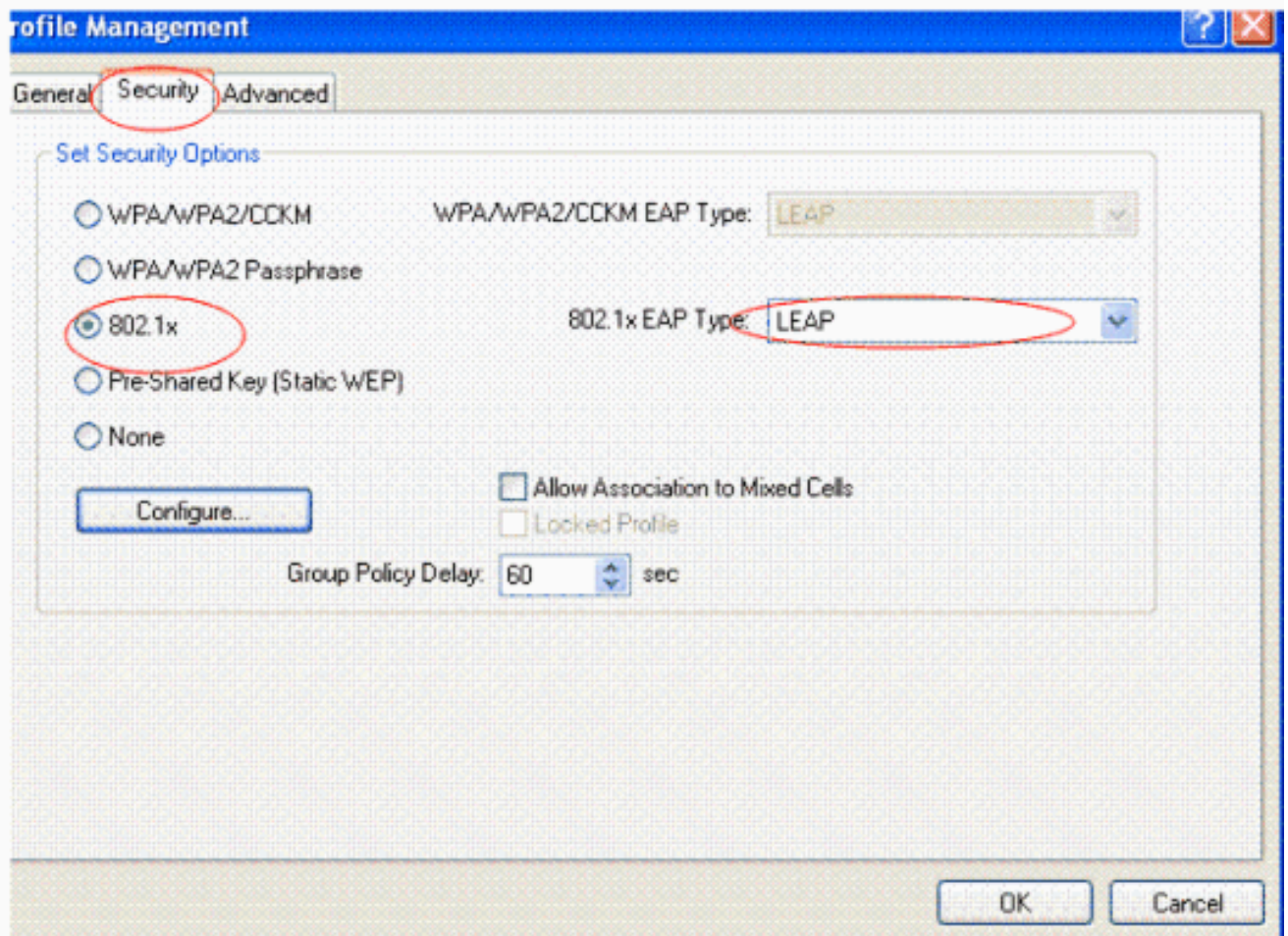
[Configuratie van draadloos clienthulpprogramma](#)

Dit document gebruikt ADU als de clientvoorziening voor de configuratie van de gebruikersprofielen. Deze configuratie gebruikt ook LEAP als het authenticatieprotocol. Configureer de ADU zoals in het voorbeeld in deze sectie wordt weergegeven.

Kies in de balk van het menu ADU **Profile Management > New** om een nieuw profiel te maken.

De voorbeeldclient is ingesteld om een deel van SSID VLAN10 te zijn. Deze diagrammen tonen hoe u een gebruikersprofiel op een client kunt configureren:





Verifiëren

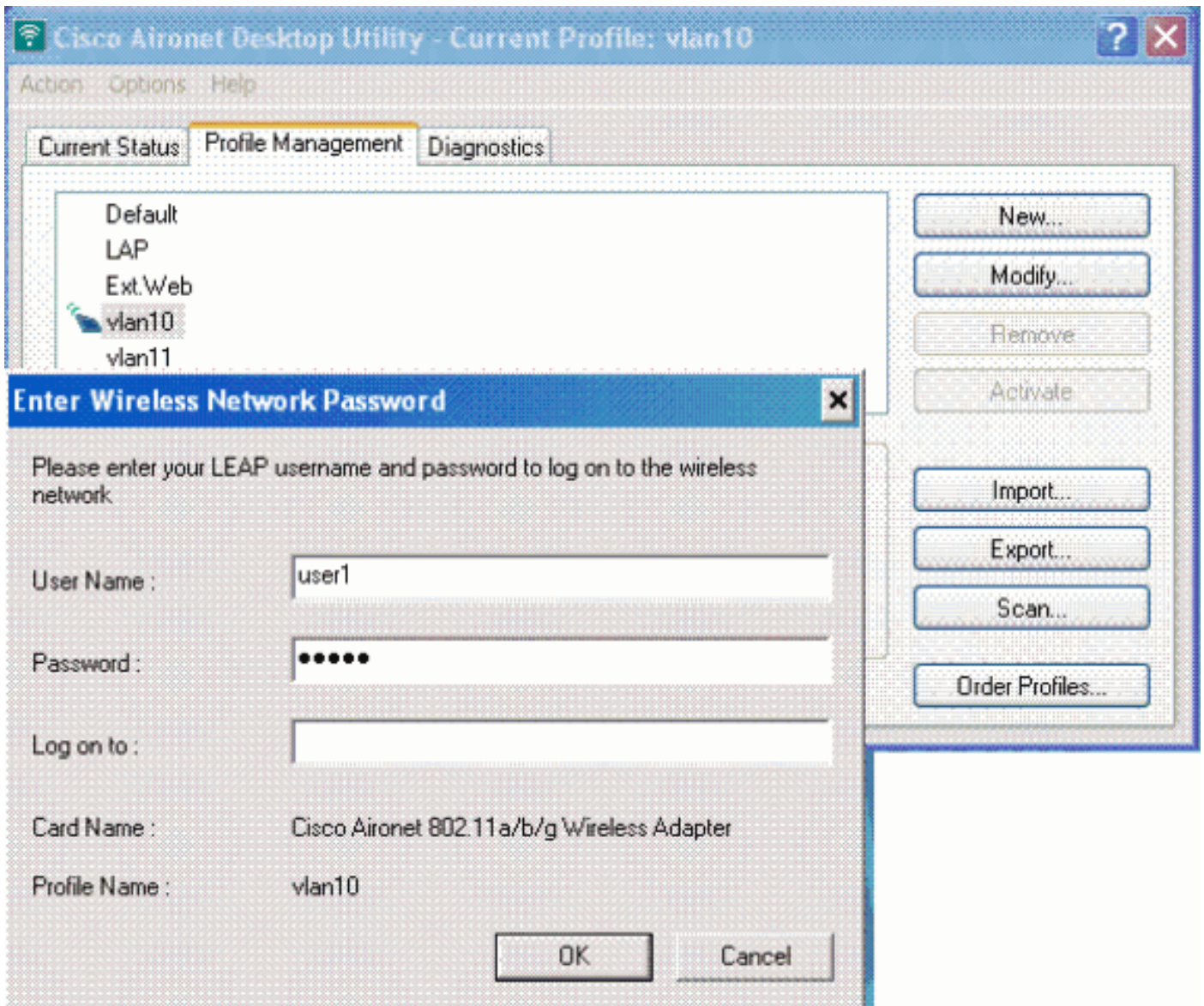
Activeert het gebruikersprofiel dat u in de automatische documentinvoer hebt ingesteld. Gebaseerd op de configuratie, wordt u gevraagd om een gebruikersnaam en wachtwoord. U kunt de ADU ook opdracht geven de gebruikersnaam en het wachtwoord van Windows voor verificatie te gebruiken. Er zijn een aantal opties waarvandaan de cliënt een echtheidscontrole kan ontvangen. U kunt deze opties configureren onder het tabblad Beveiliging > tabblad Configureren van het gebruikersprofiel dat u hebt gemaakt.

In het vorige voorbeeld, merk op dat user1 aan VLAN10 zoals gespecificeerd in de server van de RADIUS wordt toegewezen.

Dit voorbeeld gebruikt deze gebruikersnaam en wachtwoord van de clientkant om verificatie te ontvangen en toe te wijzen aan een VLAN door de RADIUS-server:

- Gebruikersnaam = gebruiker1
- Wachtwoord = gebruiker1

Dit voorbeeld toont hoe SSID VLAN10 voor de gebruikersnaam en het wachtwoord wordt gevraagd. De gebruikersnaam en het wachtwoord worden in dit voorbeeld ingevoerd:



Zodra de authenticatie en de bijbehorende validatie succesvol zijn, ontvangt u succes als het statusbericht.

Vervolgens moet u controleren of uw client is toegewezen aan het juiste VLAN zoals beschreven in de RADIUS-eigenschappen die worden verzonden. Voltooi deze stappen om dit te bereiken:

1. Kies in de GUI van de controller de optie **Draadloos > AP**.
2. Klik op **Clients** die in de linkerhoek van het venster Access Point (AP's) verschijnen. De clientstatistieken worden weergegeven.

Client MAC Addr	AP Name	WLAN Profile	Protocol	Status	Auth	Port	WGB
00:21:5c:09:08:dd	AP1130	Unknown	802.11a	Probing	No	2	No
00:21:5c:50:3a:1f	AP1130	VLAN10	802.11g	Associated	Yes	2	No

3. Klik op **Details** om de volledige details van de client te identificeren, zoals IP-adres, het VLAN waaraan deze is toegewezen, enzovoort. Dit voorbeeld toont deze details van de client,

user1:

The screenshot shows the Cisco WLC interface for monitoring a client. The 'Client Properties' section includes fields for MAC Address (00:21:50:50:3a:1f), IP Address (17.18.1.35), Client Type (Regular), User Name (User1), Port Number (2), Interface (vlan10), VLAN ID (10), CCX Version (CCXv4), E2E Version (E2Ev1), Mobility Role (Local), Mobility Peer IP Address (N/A), Policy Manager State (RUN), Mirror Mode (Disable), Management Frame Protection (No), and Security Information (Security Policy Completed: Yes, Policy Type: 802.1X, Encryption Cipher: WEP (104 bits), EAP Type: LEAP, NAC State: Access). The 'AP Properties' section includes fields for AP Address (00:15:c7:ab:55:90), AP Name (AP1130), AP Type (802.11g), WLAN Profile (VLAN10), Status (Associated), Association ID (1), 802.11 Authentication (Open System), Reason Code (0), Status Code (0), CF Pollable (Not Implemented), CF Poll Request (Not Implemented), Short Preamble (Implemented), PBCC (Not Implemented), Channel Agility (Not Implemented), Timeout (1800), and WEP State (WEP Disable).

Vanuit dit venster kunt u observeren dat deze client is toegewezen aan VLAN10 in overeenstemming met de RADIUS-eigenschappen die zijn ingesteld op de RADIUS-server. **N.B.:** Als de dynamische VLAN-toewijzing is gebaseerd op de instelling **Cisco Airespace VSA-kenmerk** zal de **interfacenaam** deze als **admin** weergeven zoals in dit voorbeeld op de pagina met clientdetails.

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

- **debug aaaa gebeurtenissen activeren**—Deze opdracht kan worden gebruikt om een succesvolle overdracht van de RADIUS-eigenschappen naar de client via de controller te waarborgen. Dit gedeelte van de debug uitvoer garandeert een succesvolle overdracht van RADIUS-kenmerken:

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[0]:
attribute 64, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[1]:
attribute 65, vendorId 0, valueLen 4
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[2]:
attribute 81, vendorId 0, valueLen 3
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[3]:
attribute 79, vendorId 0, valueLen 32
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Received EAP Attribute
(code=2, length=32,id=0) for mobile 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00000000: 02 00 00 20 11 01 00 18
4a 27 65 69 6d e4 05 f5
.....J'eim..00000010: d0 98 0c cb 1a 0c 8a 3c
.....44 a9 da 6c 36 94 0a f3 <D..l6...
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[4]:
attribute 1, vendorId 9, valueLen 16
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[5]:
attribute 25, vendorId 0, valueLen 28
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 processing avps[6]:
attribute 80, vendorId 0, valueLen 16
```

```
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Type 16777229
should be 13 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:25:08 2006: 00:40:96:ac:e6:57 Tunnel-Medium-Type 16777222
should be 6 for STA 00:40:96:ac:e6:57
Fri Jan 20 02:30:00 2006: 00:40:96:ac:e6:57 Station 00:40:96:ac:e6:57
setting dot1x reauth timeout = 1800
```

- Deze opdrachten kunnen ook nuttig zijn: **debug dot1x aaa activerendebug a-pakketten**

Problemen oplossen

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

Opmerking: Dynamische VLAN-toewijzing werkt niet voor web-verificatie door een WLC.

Gerelateerde informatie

- [EAP-verificatie met RADIUS-server](#)
- [Cisco LEAP](#)
- [Configuratie-gids voor Cisco draadloze LAN-controllers, release 4.0](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)