

Verificatie van de Lobby-beheerder van draadloze LAN-controllers via RADIUS-server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Conventies](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Configuraties](#)

[WLC-configuratie](#)

[Configuratie van RADIUS-servers](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Dit document verklaart de betrokken configuratiestappen om een lobbybeheerder van de draadloze LAN-controller (WLC) met een RADIUS-server te authenticeren.

[Voorwaarden](#)

[Vereisten](#)

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

- Kennis van het configureren van fundamentele parameters op WLC's
- Kennis van de manier waarop u een RADIUS-server kunt configureren, zoals Cisco Secure ACS
- Kennis van gastgebruikers in de WLC

[Gebruikte componenten](#)

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

- Cisco 4400 draadloze LAN-controller op versie 7.0.216.0
- Een Cisco Secure ACS dat softwareversie 4.1 draait en in deze configuratie wordt gebruikt als

een RADIUS-server.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

[Conventies](#)

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

[Achtergrondinformatie](#)

Een lobby-beheerder, ook bekend als een lobby-ambassadeur van een WLC, kan gastgebruikersaccounts maken en beheren op de draadloze LAN-controller (WLC). De lobbyambassadeur heeft beperkte configuratierechten en kan alleen toegang krijgen tot de webpagina's die gebruikt worden om de gastenrekeningen te beheren. De lobbyambassadeur kan de tijdsduur specificeren waarop de rekeningen van de gastgebruikers actief blijven. Nadat de opgegeven tijdslimiet is verstreken, worden de rekeningen van de gastgebruiker automatisch verlopen.

Raadpleeg de [implementatiegids: Cisco Guest Access Network dat de Cisco draadloze LAN-controller gebruikt](#) voor meer informatie over gastgebruikers.

Om een gastgebruikersaccount op de WLC te maken, moet u inloggen bij de controller als lobbybeheerder. Dit document verklaart hoe een gebruiker in WLC als een lobbybeheerder geauthentiseerd is op basis van de eigenschappen die door de RADIUS-server zijn geretourneerd.

Opmerking: Ook de 'Lobby'-verificatie kan worden uitgevoerd op basis van de lobbybeheerder-account die lokaal is ingesteld op de WLC. Raadpleeg [Een Lobby Ambassador-account maken](#) voor informatie over het maken van een lobby-beheeraccount op een controller.

[Configureren](#)

In deze sectie, wordt u voorgesteld van de informatie over hoe u de WLC en de Cisco Secure ACS voor het doel vormt dat in dit document wordt beschreven.

[Configuraties](#)

Dit document gebruikt deze configuraties:

- Het IP-adres van de Management Interface van WLC is 10.77.244.212/27.
- Het IP-adres van de RADIUS-server is 10.77.244.197/27.
- De gedeelde geheime sleutel die op het access point (AP) en de RADIUS server wordt gebruikt is cisco123.
- De gebruikersnaam en het wachtwoord van de lobbybeheerder in de RADIUS-server zijn beide lobbyadmin.

In het configuratievoorbeeld in dit document wordt elke gebruiker die in de controller met gebruikersnaam en wachtwoord logt als lobbybeheerder, toegewezen aan een lobbybeheerder.

[WLC-configuratie](#)

Zorg er voordat u de gewenste WLC-configuratie start voor dat de controller versie 4.0.206.0 of hoger uitvoert. Dit is te wijten aan Cisco bug-ID [CSCsg89868](#) (alleen [geregistreerde](#) klanten) waarin de webinterface van de controller verkeerde webpagina's voor de LobbyAdmin-gebruiker weergeeft wanneer de gebruikersnaam is opgeslagen in een RADIUS-database. LobbyAdmin wordt met de alleen-interface gelezen in plaats van de LobbyAdmin-interface gepresenteerd.

Dit probleem is opgelost in WLC versie 4.0.206.0. Zorg er daarom voor dat de versie van uw controller 4.0.206.0 of hoger is. Raadpleeg de [software-upgrade](#) voor [draadloze LAN-controller \(WLC\)](#) voor [informatie](#) over het upgraden van de controller naar de juiste versie.

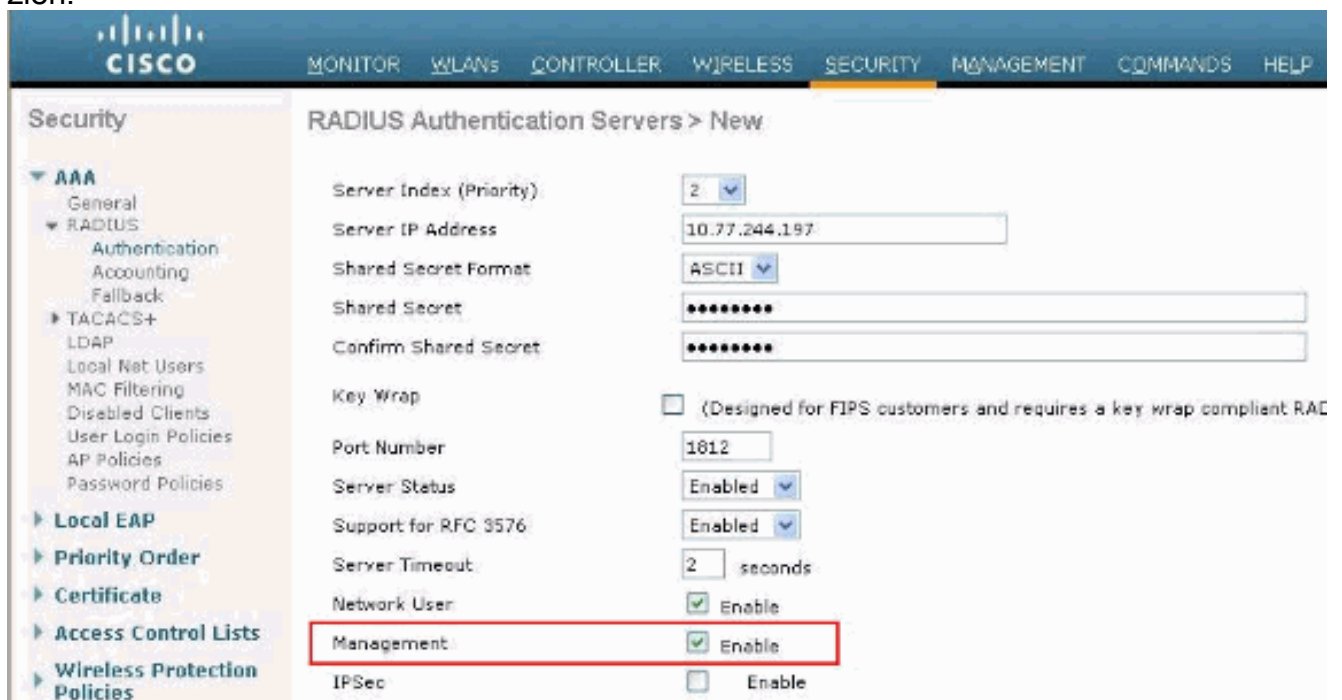
Om controllerbeheer-verificatie met de RADIUS-server uit te voeren, moet u ervoor zorgen dat de **Admin-auth-via-RADIUS**-vlag op de controller is ingeschakeld. Dit kan worden geverifieerd vanuit de opdrachtoutput van de **show Straal**.

De eerste stap is het configureren van RADIUS-serverinformatie op de controller en het instellen van Layer 3-bereikbaarheid tussen de controller en RADIUS-server.

[RADIUS-serverinformatie over de controller configureren](#)

Voltooi deze stappen om de WLC te configureren met informatie over het ACS:

1. Kies het tabblad **Beveiliging** vanuit de WLC GUI en stel het IP-adres en het gedeelde geheim van de ACS-server in. Dit gedeelde geheim moet op de ACS hetzelfde zijn zodat de WLC met de ACS kan communiceren. **Opmerking:** Het ACS gedeelde geheim is hoofdlettergevoelig. Zorg er daarom voor dat u de gedeelde geheime informatie correct invoert. Dit getal laat een voorbeeld zien:



The screenshot shows the Cisco WLC GUI with the 'Security' tab selected. The 'RADIUS Authentication Servers > New' configuration page is displayed. The 'Management' checkbox is highlighted with a red box. The configuration details are as follows:

Field	Value
Server Index (Priority)	2
Server IP Address	10.77.244.197
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RAC)
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

2. Controleer het aankruisvakje **Management** om ACS toe te staan om de WLC-gebruikers te beheren zoals in de afbeelding in stap 1. Klik vervolgens op **Toepassen**.
3. Controleer Layer 3 bereikbaarheid tussen de controller en de geconfigureerde RADIUS-server met de hulp van de **ping**-opdracht. Deze ping-optie is ook beschikbaar op de

geconfigureerde RADIUS-serverpagina in de WLC GUI in het tabblad **Security>RADIUS-verificatie**. In dit diagram wordt een succesvol ping-antwoord van de RADIUS-server weergegeven. Layer 3 bereikbaarheid is daarom beschikbaar tussen de controller en RADIUS-server.



[Configuratie van RADIUS-servers](#)

Volg de stappen in deze secties om de RADIUS-server te configureren:

1. [Voeg WLC als een AAA-client toe aan de RADIUS-server](#)
2. [Configureer de juiste RADIUS IETF-servicetype voor een lobbybeheerder](#)

[Voeg WLC als een AAA-client toe aan de RADIUS-server](#)

Voltooi deze stappen om de WLC als een AAA-client aan de RADIUS-server toe te voegen. Zoals eerder vermeld, gebruikt dit document ACS als de RADIUS-server. U kunt een RADIUS-server voor deze configuratie gebruiken.

Voltooi deze stappen om de WLC als een AAA-client in het ACS toe te voegen:

1. Kies in de ACS GUI het tabblad **Netwerkconfiguratie**.
2. Klik onder AAA-clients op **Toevoegen**.
3. Voer in het venster Add AAA Client de WLC host-naam, het IP-adres van de WLC en een gedeelte geheime sleutel in. Zie het voorbeeldschema onder stap 5.
4. Kies in het vervolgkeuzemenu Verifiëren met behulp van **RADIUS (Cisco Aironet)**.
5. Klik op **Indienen + Herstart** om de configuratie op te slaan.



Network Configuration

Add AAA Client



AAA Client Hostname	<input type="text" value="WLC2"/>
AAA Client IP Address	<input type="text" value="10.77.244.212"/>
Shared Secret	<input type="text" value="cisco123"/>
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
Authenticate Using	<input type="text" value="RADIUS (Cisco Aironet)"/>
<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	

[Configureer de juiste RADIUS IETF-servicetype voor een lobbybeheerder](#)

Om een beheergebruiker van een controller als lobby-beheerder via de RADIUS-server te authentifieren, moet u de gebruiker aan de RADIUS-database toevoegen met de IETF RADIUS-servicetype die aan **Callback Administration** is ingesteld. Deze eigenschap wijst de specifieke gebruiker de rol toe van een lobbybeheerder op een controller.

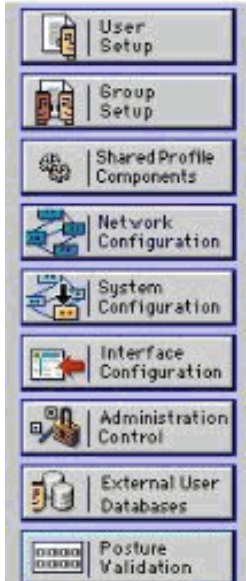
Dit document toont de voorbeeldgebruiker lobbyadmin als lobbybeheerder. Voltooi de volgende stappen op de ACS om deze gebruiker te configureren:

1. Kies in de ACS GUI het tabblad **Gebruikersinstelling**.
2. Voer de gebruikersnaam in die aan de ACS moet worden toegevoegd zoals in dit voorbeeldvenster wordt weergegeven:



User Setup

Select



User:

List users beginning with letter/number:

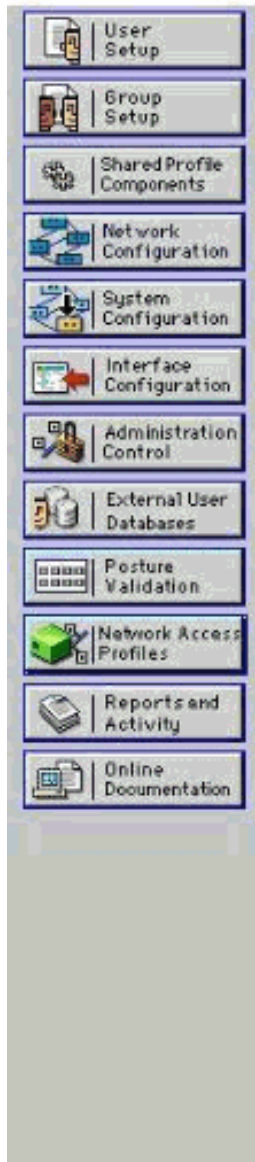
A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9			

3. Klik op **Toevoegen/bewerken** om naar de pagina met gebruikersbewerking te gaan.
4. Typ in de pagina Bewerken door gebruiker de gegevens Naam, Beschrijving en wachtwoord van deze gebruiker. In dit voorbeeld zijn de gebruikersnaam en het wachtwoord beide lobbyadmin.



User Setup

User: lobbyadmin (New User)



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

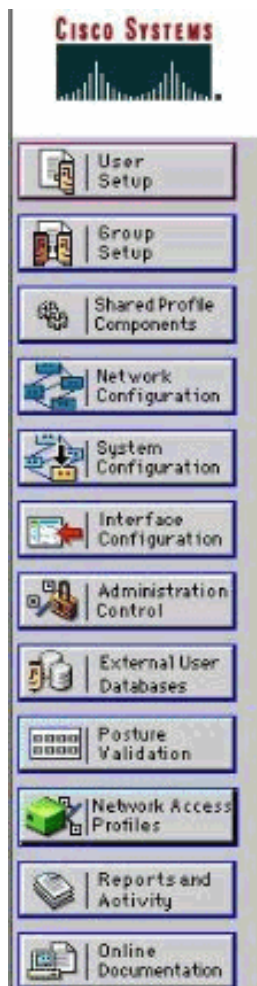
Separate (CHAP/MS-CHAP/ARAP)

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 authentication is enabled.

5. Scroll naar de instelling RADIUS-kenmerken van IETF en controleer het aankruisvakje **Service-Type Kenmerk**.
6. Kies **Terugbellen** administratief in het keuzemenu Service-Type en klik op **Indienen**. Dit is de eigenschap die deze gebruiker de rol van een lobbybeheerder toekent.



User Setup

Account Disable ?

Never

Disable account if:

Date exceeds: Sep 25 2011

Failed attempts exceed: 5

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

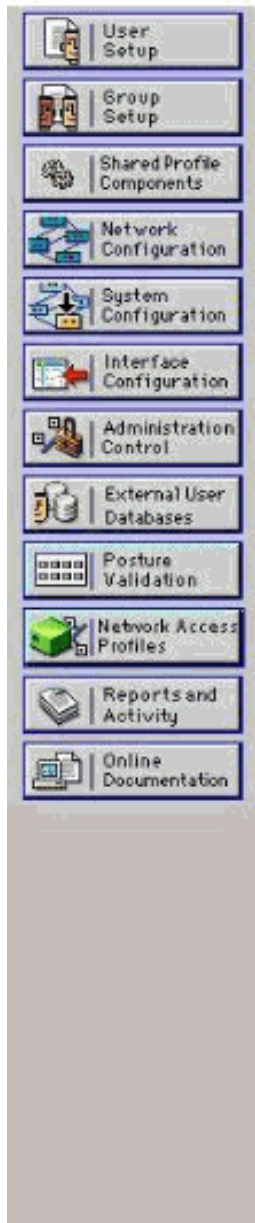
IETF RADIUS Attributes ?

[006] Service-Type Callback Administrative

Soms is deze eigenschap Service-Type niet zichtbaar onder de gebruikersinstellingen. In dat geval moeten deze stappen worden voltooid om het zichtbaar te maken: Selecteer in de ACS GUI de optie **Interface Configuration > RADIUS (IETF)** om de IETF-eigenschappen in het User Configuration-venster in te schakelen. Dit brengt u naar de pagina met RADIUS-instellingen (IETF). Via de pagina RADIUS (IETF)-instellingen kunt u de IETF-eigenschap inschakelen die bij gebruikers- of groepsinstellingen zichtbaar moet zijn. Voor deze configuratie, controleer **het servicetype** voor de gebruikerskolom en klik op **Indienen**. Dit venster toont een voorbeeld:



Interface Configuration



RADIUS (IETF)

User	Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> [006] Service-Type
<input type="checkbox"/>	<input checked="" type="checkbox"/> [007] Framed-Protocol
<input type="checkbox"/>	<input checked="" type="checkbox"/> [009] Framed-IP-Netmask
<input type="checkbox"/>	<input checked="" type="checkbox"/> [010] Framed-Routing
<input type="checkbox"/>	<input checked="" type="checkbox"/> [011] Filter-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [012] Framed-MTU
<input type="checkbox"/>	<input checked="" type="checkbox"/> [013] Framed-Compression
<input type="checkbox"/>	<input checked="" type="checkbox"/> [014] Login-IP-Host
<input type="checkbox"/>	<input checked="" type="checkbox"/> [015] Login-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [016] Login-TCP-Port
<input type="checkbox"/>	<input checked="" type="checkbox"/> [018] Reply-Message
<input type="checkbox"/>	<input checked="" type="checkbox"/> [020] Callback-Id
<input type="checkbox"/>	<input checked="" type="checkbox"/> [022] Framed-Route
<input type="checkbox"/>	<input checked="" type="checkbox"/> [023] Framed-IPX-Network
<input type="checkbox"/>	<input checked="" type="checkbox"/> [024] State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [025] Class
<input type="checkbox"/>	<input checked="" type="checkbox"/> [027] Session-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [028] Idle-Timeout
<input type="checkbox"/>	<input checked="" type="checkbox"/> [029] Termination-Action
<input type="checkbox"/>	<input checked="" type="checkbox"/> [033] Proxy-State
<input type="checkbox"/>	<input checked="" type="checkbox"/> [034] Login-LAT-Service
<input type="checkbox"/>	<input checked="" type="checkbox"/> [035] Login-LAT-Node
<input type="checkbox"/>	<input checked="" type="checkbox"/> [036] Login-LAT-Group

Opmerking: Dit voorbeeld specificeert authenticatie per gebruiker. U kunt ook verificatie uitvoeren op basis van de groep waartoe een bepaalde gebruiker behoort. In dergelijke gevallen controleert u het aanvinkvakje **Group** zodat deze eigenschap onder Groepsinstellingen zichtbaar is. **Opmerking:** Als de authenticatie op groepsbasis plaatsvindt, moet u gebruikers toewijzen aan een bepaalde groep en de IETF-eigenschappen groepsinstelling configureren om toegangsrechten te geven aan gebruikers van die groep. Raadpleeg [Gebruikersgroepsbeheer](#) voor uitgebreide informatie over de manier waarop u groepen kunt configureren en beheren.

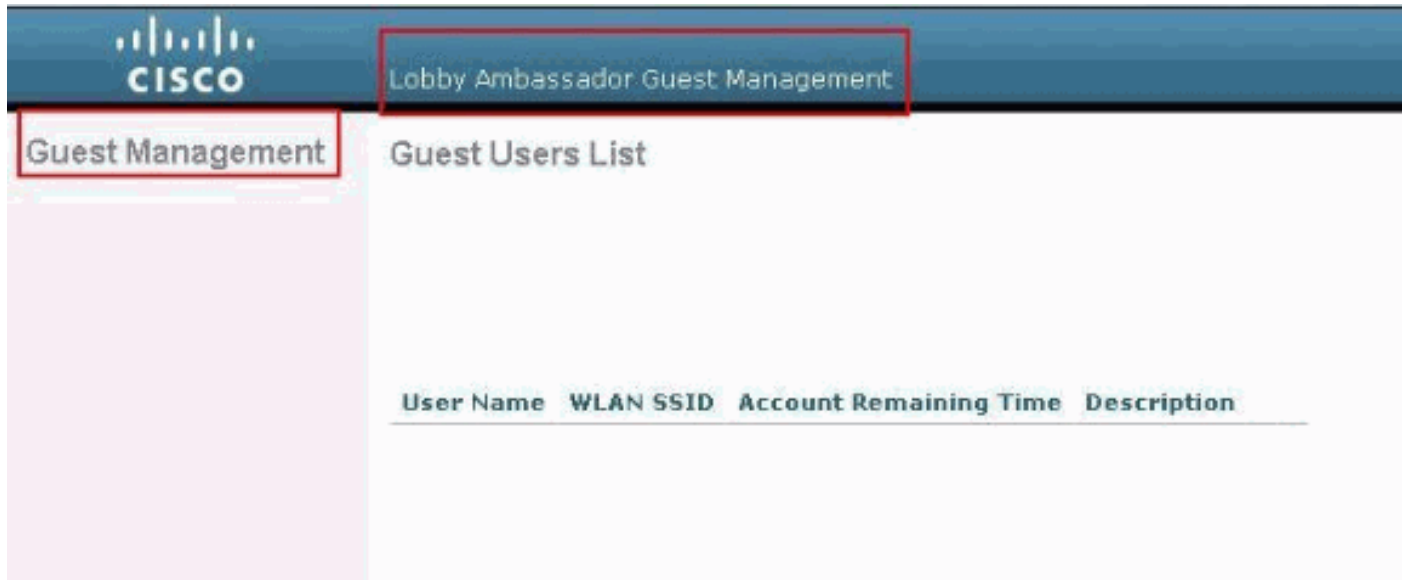
Verifiëren

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

Om te verifiëren dat uw configuratie naar behoren werkt, heeft u toegang tot de WLC via de GUI (HTTP/HTTPS) modus.

Opmerking: Een lobbyambassadeur kan geen toegang hebben tot de CLI-interface van de controller en kan daarom alleen gastgebruikersrekeningen maken vanuit de GUI van de controller.

Wanneer de loginmelding wordt weergegeven, typt u de gebruikersnaam en het wachtwoord zoals ingesteld in het ACS. Als de configuraties correct zijn, wordt u als **lobbybeheerder** geauthentiseerd in de WLC. Dit voorbeeld laat zien hoe de GUI van een lobbybeheerder voor succesvolle authenticatie zorgt:



Opmerking: U kunt zien dat een lobbybeheerder geen andere optie heeft dan het beheer van de gastgebruiker.

Om het vanuit de CLI-modus te controleren, heeft telnet in de controller als een gelezen-schrijfbeheerder plaatsgevonden. Geef de **debug aaa** uit om opdracht te geven bij de controller CLI.

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

```
(Cisco Controller) >
```

```
*aaaQueueReader: Aug 26 18:07:35.072: ReProcessAuthentication previous proto 28,
next proto 20001
*aaaQueueReader: Aug 26 18:07:35.072: AuthenticationRequest: 0x3081f7dc
*aaaQueueReader: Aug 26 18:07:35.072: Callback.....0x10756dd0
*aaaQueueReader: Aug 26 18:07:35.072: protocolType.....0x00020001
*aaaQueueReader: Aug 26 18:07:35.072:
proxyState.....00:00:00:40:
00:00-00:00
*aaaQueueReader: Aug 26 18:07:35.072: Packet contains 5 AVPs (not shown)
*aaaQueueReader: Aug 26 18:07:35.072: apfVapRadiusInfoGet: WLAN(0) dynamic int attributes
srcAddr:
0x0, gw:0x0, mask:0x0, vlan:0, dpPort:0, srcPort:0
*aaaQueueReader: Aug 26 18:07:35.073: 00:00:00:40:00:00 Successful transmission of
Authentication
Packet (id 39) to 10.77.244.212:1812, proxy state 00:00:00:40:00:00-00:01
*aaaQueueReader: Aug 26 18:07:35.073: 00000000: 01 27 00 47 00 00 00 00 00 00 00 00 00 00 00 00
..'.G.....
*aaaQueueReader: Aug 26 18:07:35.073: 00000010: 00 00 00 00 01 0c 6c 6f 62 62 79 61 64 6d 69 6e
.....lobbyadmin
*aaaQueueReader: Aug 26 18:07:35.073: 00000020: 02 12 5f 5b 5c 12 c5 c8 52 d3 3f 4f 4f 8e 9d 38
.._[\...R.?00..8
*aaaQueueReader: Aug 26 18:07:35.073: 00000030: 42 91 06 06 00 00 00 07 04 06 0a 4e b1 1a 20 09
```

```

B.....N....
*aaaQueueReader: Aug 26 18:07:35.073: 00000040: 57 4c 43 34 34 30 30 WLC4400
*radiusTransportThread: Aug 26 18:07:35.080: 00000000: 02 27 00 40 7e 04 6d 533d ed 79 9c b6 99
d1
f8  .'.@~.mS=.y.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000010: d0 5a 8f 4f 08 06 ff ffff ff 06 06 00 00
00
0b  .Z.O.....
*radiusTransportThread: Aug 26 18:07:35.080: 00000020: 19 20 43 41 43 53 3a 302f 61 65 32 36 2f
61
34  ..CACS:0/ae26/a4
*radiusTransportThread: Aug 26 18:07:35.080: 00000030: 65 62 31 31 61 2f 6c 6f62 62 79 61 64 6d
69
6e  eb11a/lobbyadmin
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processIncomingMessages: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: ****Enter processRadiusResponse: response code=2
*radiusTransportThread: Aug 26 18:07:35.080: 00:00:00:40:00:00 Access-Accept received from
RADIUS
server 10.77.244.212 for mobile 00:00:00:40:00:00 receiveId = 0
*radiusTransportThread: Aug 26 18:07:35.080: AuthorizationResponse: 0x13c73d50
*radiusTransportThread: Aug 26 18:07:35.080:      structureSize.....118
*radiusTransportThread: Aug 26 18:07:35.080:      resultCode.....0
*radiusTransportThread: Aug 26 18:07:35.080:
protocolUsed.....0x00000001
*radiusTransportThread: Aug 26 18:07:35.080:
proxyState.....00:00:00:40:00:00-00:00
*radiusTransportThread: Aug 26 18:07:35.080:      Packet contains 3 AVPs:
*radiusTransportThread: Aug 26 18:07:35.080:          AVP[01] Framed-IP-
Address.....0xffffffff (-1) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:          AVP[02] Service-
Type.....0x0000000b (11) (4 bytes)
*radiusTransportThread: Aug 26 18:07:35.080:          AVP[03]
Class.....
CACS:0/ae26/a4eb11a/lobbyadmin (30 bytes)
*emWeb: Aug 26 18:07:35.084: Authentication succeeded for lobbyadmin

```

In de gemarkeerde informatie in deze uitvoer kunt u zien dat het servicetype attribuut 11 (Callback Administration) wordt doorgegeven aan de controller op de ACS-server en dat de gebruiker wordt inlogd als lobbybeheerder.

Deze opdrachten kunnen extra hulp opleveren:

- automatisch fout Herstel uitvoeren
- debug aaaaathedingen activeren
- debug a-pakketten

Opmerking: Raadpleeg [Belangrijke informatie over debug Commands](#) voordat u debug-opdrachten gebruikt.

[Problemen oplossen](#)

Als u inlogt bij een controller met de rechten van de lobbyambassadeur, kunt u geen gastgebruikersaccount met een levenslange waarde van "0" maken, een account die nooit vervalst. In deze situaties kan de levenswaarde niet de 0-foutmelding zijn.

Dit is te wijten aan Cisco bug-ID [CSCsf32392](#) (alleen [geregistreerde](#) klanten), die voornamelijk voorkomt bij WLC versie 4.0. Dit probleem is opgelost in WLC versie 4.1.

Gerelateerde informatie

- [RADIUS-serververificatie van beheergebruikers in het configuratievoorbeeld van de controller](#)
- [Cisco Unified Wireless Network TACACS+ configuratie](#)
- [Cisco-configuratiegids voor draadloze LAN-controllers, release 4.0 - gebruikersaccounts beheren](#)
- [Configuratievoorbeeld van ACL's op draadloze LAN-controllers](#)
- [WLC FAQ \(draadloze LAN-controller\)](#)
- [ACL's op draadloze LAN-controllers: Regels, beperkingen en voorbeelden](#)
- [Configuratievoorbeeld voor externe webverificatie met draadloze LAN-controllers](#)
- [Configuratievoorbeeld van draadloze LAN-controllers](#)
- [Gast WLAN en interne WLAN-toepassing met WLC-configuratievoorbeeld](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)