

RADIUS 서버를 통한 무선 LAN 컨트롤러 로비 관리자 인증

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[배경 정보](#)

[구성](#)

[구성](#)

[WLC 컨피그레이션](#)

[RADIUS 서버 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 RADIUS 서버를 사용하여 WLC(무선 LAN 컨트롤러)의 로비 관리자를 인증하는 데 필요한 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC에서 기본 매개변수를 구성하는 방법에 대한 지식
- Cisco Secure ACS와 같은 RADIUS 서버를 구성하는 방법에 대한 지식
- WLC의 게스트 사용자 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 7.0.216.0을 실행하는 Cisco 4400 Wireless LAN Controller
- 소프트웨어 버전 4.1을 실행하고 이 컨피그레이션에서 RADIUS 서버로 사용되는 Cisco Secure ACS입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

[표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

[배경 정보](#)

WLC의 로비 대사라고도 하는 로비 관리자는 WLC(Wireless LAN Controller)에서 게스트 사용자 계정을 생성하고 관리할 수 있습니다. 로비 대사는 제한된 구성 권한을 가지며 게스트 어카운트 관리에 사용되는 웹 페이지만 액세스할 수 있습니다. 로비 대사는 게스트 사용자 계정이 활성 상태로 유지되는 시간을 지정할 수 있습니다. 지정된 시간이 경과하면 게스트 사용자 계정이 자동으로 만료됩니다.

구축 [설명서 참조](#): [Cisco Guest Access Using the Cisco Wireless LAN Controller\(Cisco Wireless LAN Controller\)](#)를 사용하여 게스트 사용자에 대한 자세한 정보)

WLC에서 게스트 사용자 계정을 생성하려면 컨트롤러 관리자로 컨트롤러에 로그인해야 합니다. 이 문서에서는 RADIUS 서버에서 반환한 특성을 기반으로 사용자를 로비 관리자로 WLC에 인증하는 방법에 대해 설명합니다.

참고: 로비 관리자 인증은 WLC에 로컬로 구성된 로비 관리자 계정을 기반으로 수행할 수도 있습니다. 컨트롤러 [에서 로컬로 로비 관리자](#) 계정을 만드는 방법에 대한 자세한 내용은 로비 앰버서더 계정 만들기를 참조하십시오.

[구성](#)

이 섹션에서는 이 문서에 설명된 용도로 WLC 및 Cisco Secure ACS를 구성하는 방법에 대한 정보를 제공합니다.

[구성](#)

이 문서에서는 다음 구성을 사용합니다.

- WLC의 관리 인터페이스 IP 주소는 10.77.244.212/27입니다.
- RADIUS 서버의 IP 주소는 10.77.244.197/27입니다.
- 액세스 포인트(AP) 및 RADIUS 서버에서 사용되는 공유 비밀 키는 cisco123입니다.
- RADIUS 서버에 구성된 로비 관리자의 사용자 이름과 비밀번호는 lobbyadmin입니다.

이 문서의 컨피그레이션 예에서는 lobbyadmin으로 사용자 이름과 비밀번호를 사용하여 컨트롤러에 로그인하는 모든 사용자에게 로비 관리자 역할이 할당됩니다.

[WLC 컨피그레이션](#)

필요한 WLC 컨피그레이션을 시작하기 전에 컨트롤러가 버전 4.0.206.0 이상을 실행하는지 확인하십시오. 이는 Cisco 버그 ID [CSCsg89868\(등록된 고객만 해당\)](#) 때문입니다. 이 경우 사용자 이름이 RADIUS 데이터베이스에 저장될 때 컨트롤러의 웹 인터페이스에 LobbyAdmin 사용자에게 대한 잘못된 웹 페이지가 표시됩니다. LobbyAdmin 인터페이스에는 LobbyAdmin 인터페이스 대신 ReadOnly

인터페이스가 제공됩니다.

이 버그는 WLC 버전 4.0.206.0에서 확인되었습니다. 따라서 컨트롤러 버전이 4.0.206.0 이상인지 확인하십시오. 컨트롤러를 적절한 버전으로 업그레이드하는 방법에 대한 지침은 [WLC\(Wireless LAN Controller\) 소프트웨어 업그레이드](#)를 참조하십시오.

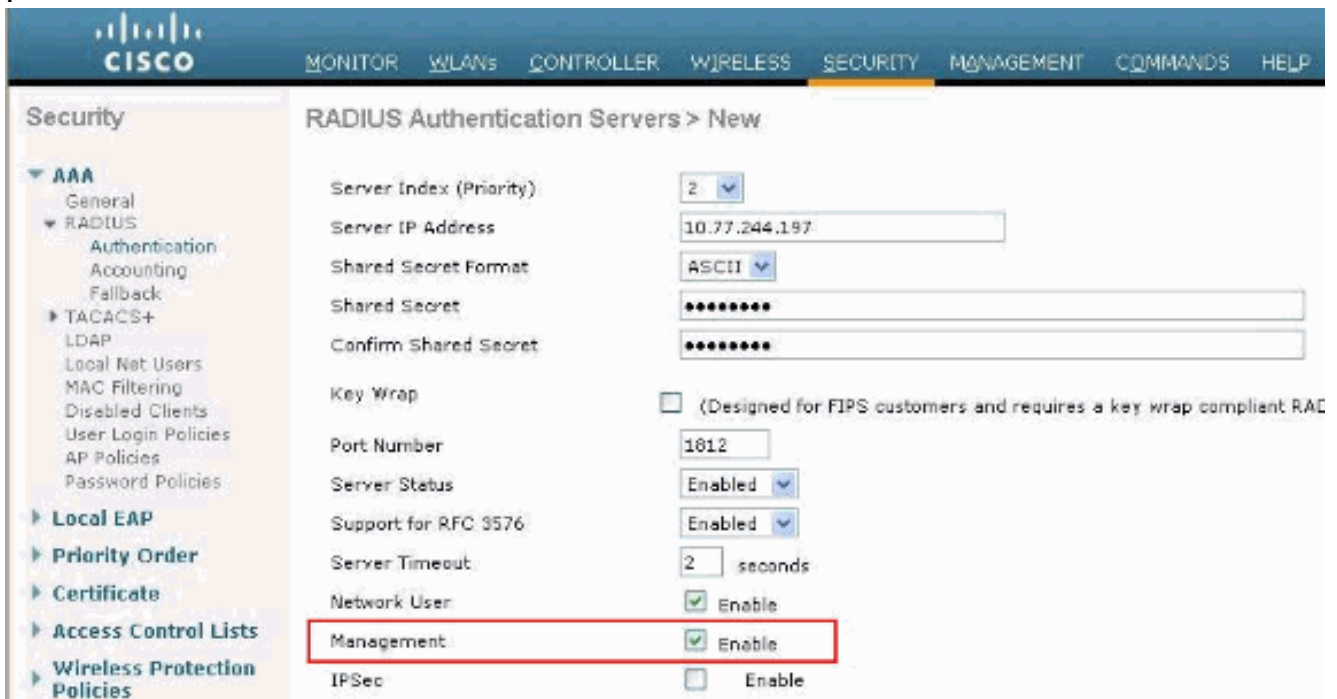
RADIUS 서버와의 컨트롤러 관리 인증을 수행하려면 컨트롤러에서 Admin-auth-via-RADIUS 플래그가 활성화되었는지 확인합니다. 이는 show radius summary 명령 출력에서 확인할 수 있습니다.

첫 번째 단계는 컨트롤러에서 RADIUS 서버 정보를 구성하고 컨트롤러와 RADIUS 서버 간에 레이어 3 연결성을 설정하는 것입니다.

컨트롤러에서 RADIUS 서버 정보 구성

ACS에 대한 세부 정보로 WLC를 구성하려면 다음 단계를 완료합니다.

1. WLC GUI에서 **Security(보안)** 탭을 선택하고 ACS 서버의 IP 주소 및 공유 암호를 구성합니다. WLC가 ACS와 통신하려면 이 공유 암호가 ACS에서 동일해야 합니다. **참고:** ACS 공유 암호는 대/소문자를 구분합니다. 따라서 공유 암호 정보를 올바르게 입력해야 합니다. 다음 그림은 예를 보여줍니다



2. ACS가 1단계의 그림과 같이 WLC 사용자를 관리할 수 있도록 하려면 **Management** 확인란을 선택하고 Apply를 클릭합니다.
3. ping 명령의 도움을 받아 컨트롤러와 구성된 RADIUS 서버 간의 레이어 3 연결성을 확인합니다. 이 ping 옵션은 WLC GUI의 Security(보안) > RADIUS Authentication(RADIUS 인증) 탭에서 구성된 RADIUS 서버 페이지에서도 사용할 수 있습니다. 이 다이어그램은 RADIUS 서버에서 성공적으로 ping 응답을 한 것을 보여줍니다. 따라서 컨트롤러와 RADIUS 서버 간에 레이어 3 연결성을 사용할 수 있습니다



[RADIUS 서버 구성](#)

RADIUS 서버를 구성하려면 다음 섹션의 단계를 완료합니다.

1. [RADIUS 서버에 AAA 클라이언트로 WLC 추가](#)
2. [로비 관리자에 대한 적절한 RADIUS IETF 서비스 유형 특성 구성](#)

[RADIUS 서버에 AAA 클라이언트로 WLC 추가](#)

RADIUS 서버에서 WLC를 AAA 클라이언트로 추가하려면 다음 단계를 완료합니다. 앞에서 언급한 대로 이 문서에서는 ACS를 RADIUS 서버로 사용합니다. 이 컨피그레이션에 RADIUS 서버를 사용할 수 있습니다.

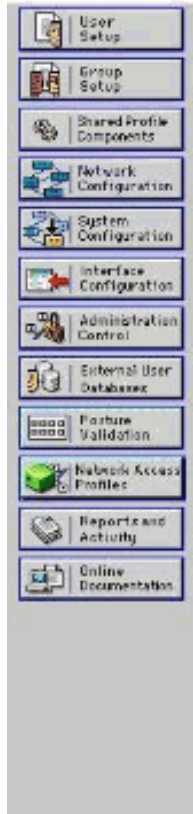
ACS에서 WLC를 AAA 클라이언트로 추가하려면 다음 단계를 완료합니다.

1. ACS GUI에서 **Network Configuration** 탭을 선택합니다.
2. AAA Clients(AAA 클라이언트)에서 Add **Entry(항목 추가)**를 클릭합니다.
3. Add AAA Client(AAA 클라이언트 추가) 창에서 WLC 호스트 이름, WLC의 IP 주소 및 공유 비밀번호 키를 입력합니다. 5단계의 예제 다이어그램을 참조하십시오.
4. Authenticate Using(다음을 사용하여 인증) 드롭다운 메뉴에서 **RADIUS(Cisco Aironet)**를 선택합니다.
5. 구성을 저장하려면 **Submit + Restart**를 클릭합니다



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	

[로비 관리자에 대한 적절한 RADIUS IETF 서비스 유형 특성 구성](#)

RADIUS 서버를 통해 컨트롤러의 관리 사용자를 로비 관리자로 인증하려면 IETF RADIUS Service-Type 특성이 **Callback Administrative**로 설정된 RADIUS 데이터베이스에 사용자를 추가해야 합니다. 이 속성은 특정 사용자에게 컨트롤러에서 로비 관리자 역할을 할당합니다.

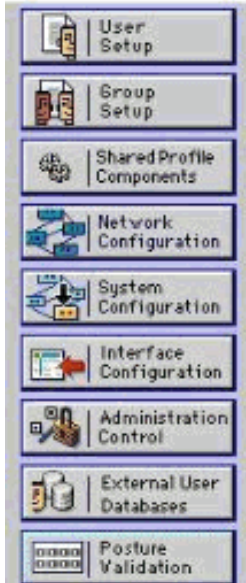
이 문서에서는 로비 관리자로서의 사용자 lobbyadmin 예를 보여줍니다. 이 사용자를 구성하려면 ACS에서 다음 단계를 완료하십시오.

1. ACS GUI에서 **User Setup** 탭을 선택합니다.
2. 다음 예제 창에 표시된 대로 ACS에 추가할 사용자 이름을 입력합니다



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. 사용자 **편집** 페이지로 이동하려면 추가/편집을 누릅니다.
4. 사용자 편집 페이지에서 이 사용자의 실제 이름, 설명 및 비밀번호 세부 정보를 제공합니다.이 예에서 사용된 사용자 이름과 비밀번호는 lobbyadmin입니다



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.

- 아래로 스크롤하여 IETF RADIUS Attributes(IETF RADIUS 특성) 설정으로 이동하고 Service-Type Attribute(서비스 유형 특성) 확인란을 선택합니다.
- 서비스 유형 풀다운 메뉴에서 콜백 관리를 선택하고 제출을 누릅니다. 이 사용자에게 로비 관리자의 역할을 할당하는 속성입니다

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

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

경우에 따라 이 Service-Type 특성은 사용자 설정에 표시되지 않습니다. 이 경우 다음 단계를 완료하여 이 단계를 표시하십시오. ACS GUI에서 Interface Configuration(인터페이스 컨피그레이션) > RADIUS(IETF)를 선택하여 User Configuration(사용자 컨피그레이션) 창에서 IETF 특성을 활성화합니다. 그러면 RADIUS(IETF) 설정 페이지로 이동합니다. RADIUS (IETF) 설정 페이지에서 사용자 또는 그룹 설정 아래에 표시되어야 하는 IETF 특성을 활성화할 수 있습니다. 이 컨피그레이션에서는 **User**(사용자) 열에 대해 Service-Type(서비스 유형)을 선택하고 Submit(제출)을 클릭합니다. 이 창에는 다음 예가 표시됩니다



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

참고: 이 예에서는 사용자별로 인증을 지정합니다. 특정 사용자가 속한 그룹을 기반으로 인증을 수행할 수도 있습니다. 이러한 경우 그룹 설정 아래에 이 속성이 표시되도록 **그룹** 확인란을 선택합니다. **참고:** 또한 인증이 그룹 기반인 경우 특정 그룹에 사용자를 할당하고 그룹 설정 IETF 속성을 구성하여 해당 그룹의 사용자에게 액세스 권한을 제공해야 합니다. 그룹 구성 및 관리 방법에 대한 자세한 내용은 [사용자 그룹 관리](#)를 참조하십시오.

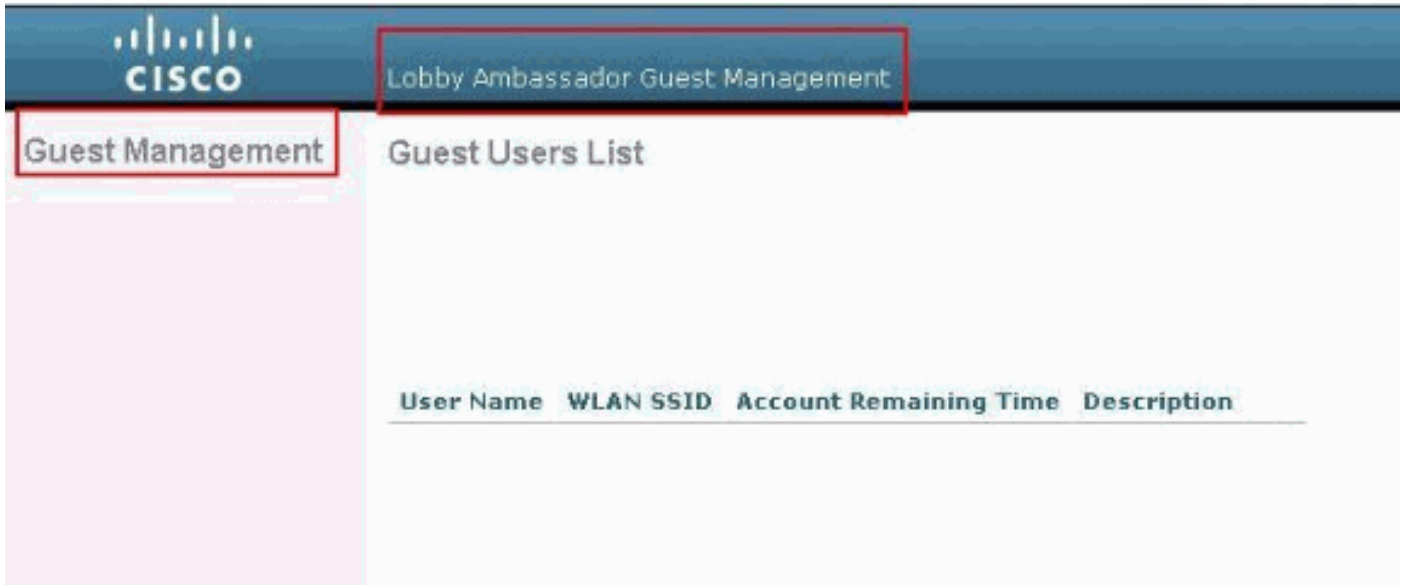
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

컨피그레이션이 제대로 작동하는지 확인하려면 GUI(HTTP/HTTPS) 모드를 통해 WLC에 액세스합니다.

참고: 로비 앰버서더는 컨트롤러 CLI 인터페이스에 액세스할 수 없으므로 컨트롤러 GUI에서만 게스트 사용자 계정을 생성할 수 있습니다.

로그인 프롬프트가 나타나면 ACS에 구성된 사용자 이름과 비밀번호를 입력합니다.컨피그레이션이 올바른 경우 WLC에서 로비 관리자로 인증됩니다.다음 예에서는 로비 관리자의 GUI가 성공적인 인증 후 어떻게 작동하는지 보여줍니다.



참고: 로비 관리자는 게스트 사용자 관리 외에 다른 옵션이 없음을 확인할 수 있습니다.

CLI 모드에서 확인하기 위해 컨트롤러에 읽기-쓰기 관리자로 텔넷합니다.컨트롤러 CLI에서 **debug aaa all enable** 명령을 실행합니다.

```
(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

```

이 출력의 강조 표시된 정보에서 서비스 유형 특성 11(콜백 관리)이 ACS 서버에서 컨트롤러에 전달되고 사용자가 로비 관리자로 로그인되어 있음을 확인할 수 있습니다.

다음 명령은 추가 도움일 수 있습니다.

- 디버그 aaa 세부사항 활성화
- 디버그 aaa 이벤트 활성화
- 디버그 aaa 패킷 활성화

참고: debug 명령을 사용하기 전에 디버그 [명령에 대한 중요 정보](#)를 참조하십시오.

문제 해결

로비 앰버서더 권한으로 컨트롤러에 로그인할 때 만료되지 않은 어카운트인 "0" 수명 값으로 게스트 사용자 어카운트를 생성할 수 없습니다. 이러한 경우 Lifetime 0 오류 메시지 .

이는 Cisco 버그 ID CSCsf32392([등록된](#) 고객만 해당)로 주로 WLC 버전 4.0에 있습니다. 이 버그는 WLC 버전 4.1에서 해결되었습니다.

관련 정보

- [컨트롤러 컨피그레이션에서 관리 사용자의 RADIUS 서버 인증 예](#)
- [Cisco Unified Wireless Network TACACS+ 컨피그레이션](#)
- [Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 4.0 - 사용자 계정 관리](#)
- [무선 LAN 컨트롤러 컨피그레이션의 ACL 예](#)
- [WLC\(Wireless LAN Controller\) FAQ](#)

- [무선 LAN 컨트롤러의 ACL: 규칙, 제한 사항 및 예](#)
- [무선 LAN 컨트롤러를 사용한 외부 웹 인증 컨피그레이션 예](#)
- [무선 LAN 컨트롤러 웹 인증 컨피그레이션 예](#)
- [WLC를 사용하는 게스트 WLAN 및 내부 WLAN 컨피그레이션 예](#)
- [기술 지원 및 문서 - Cisco Systems](#)