

# مكحت ةدحوب صاخلا وهبلا لوؤسم ةقداصم مداخ ربع ةيكلساللا ةيلحمللا ةكبشللا RADIUS

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[معلومات أساسية](#)

[التكوين](#)

[التكوينات](#)

[تكوين وحدة التحكم في شبكة LAN اللاسلكية \(WLC\)](#)

[تكوين خادم RADIUS](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## [المقدمة](#)

يشرح هذا المستند خطوات التكوين المعنية لمصادقة مسؤول البهو لوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام خادم RADIUS.

## [المتطلبات الأساسية](#)

### [المتطلبات](#)

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- معرفة كيفية تكوين المعلمات الأساسية على WLCs
- معرفة كيفية تكوين خادم RADIUS، مثل ACS الآمن من Cisco
- معرفة المستخدمين الضيوف في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

### [المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم في شبكة LAN اللاسلكية Cisco 4400 التي تشغل الإصدار 7.0.216.0

• مصدر المحتوى الإضافي الآمن من Cisco الذي يشغل الإصدار 4.1 من البرنامج ويتم استخدامه كخادم RADIUS في هذا التكوين.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## معلومات أساسية

يمكن لمسؤول البهو، المعروف أيضا باسم سفير البهو الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، إنشاء حسابات المستخدمين الضيوف وإدارتها على وحدة التحكم في الشبكة المحلية اللاسلكية (WLC). يتمتع سفير مجموعة الضغط بامتيازات تكوين محدودة ويمكنه الوصول فقط إلى صفحات الويب المستخدمة لإدارة حسابات الضيوف. يمكن لسفير مجموعة الضغط تحديد مقدار الوقت الذي تبقى فيه حسابات المستخدمين الضيوف نشطة. بعد انقضاء الوقت المحدد، تنتهي صلاحية حسابات المستخدمين الضيوف تلقائيا.

ارجع إلى [دليل النشر: Cisco Guest Access باستخدام وحدة التحكم في الشبكة المحلية اللاسلكية من Cisco](#) للحصول على مزيد من المعلومات حول المستخدمين الضيوف.

من أجل إنشاء حساب مستخدم ضيف على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يلزمك تسجيل الدخول إلى وحدة التحكم كمسؤول باللوحة. يشرح هذا المستند كيفية مصادقة مستخدم في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كمسؤول بساحة تحكم استنادا إلى السمات التي يتم إرجاعها بواسطة خادم RADIUS.

**ملاحظة:** يمكن أيضا إجراء مصادقة مسؤول البهو استنادا إلى حساب مسؤول البهو الذي تم تكوينه محليا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). ارجع إلى [إنشاء حساب سفير باللوحة مفاتيح](#) للحصول على معلومات حول كيفية إنشاء حساب مسؤول باللوحة محليا على وحدة تحكم.

## التكوين

في هذا القسم، تقدم لك معلومات حول كيفية تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) و Cisco ACS الآمن للغرض الموضح في هذا المستند.

## التكوينات

يستخدم هذا المستند التكوينات التالية:

• عنوان IP الخاص بواجهة الإدارة الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) هو 27/10.77.244.212.

• عنوان IP الخاص بخادم RADIUS هو 27/10.77.244.197.

• المفتاح السري المشترك الذي يتم استخدامه على نقطة الوصول (AP) وخادم RADIUS هو Cisco123.

• اسم المستخدم وكلمة المرور الخاصة بمسؤول البهو الذي تم تكوينه في خادم RADIUS هما كلا من LOBBYADMIN.

في مثال التكوين في هذا المستند، يتم تعيين دور مسؤول البهو إلى أي مستخدم يقوم بتسجيل الدخول إلى وحدة التحكم باسم المستخدم وكلمة المرور كمسؤول جماعة ضغط.

## تكوين وحدة التحكم في شبكة LAN اللاسلكية (WLC)

قبل بدء تكوين WLC الضروري، تأكد من أن وحدة التحكم لديك تشغل الإصدار 4.0.206.0 أو إصدار أحدث. وهذا يرجع إلى معرف تصحيح الأخطاء من [CSCsg89868](#) Cisco ([العملاء المسجلون](#) فقط) حيث تعرض واجهة ويب لوحدة التحكم صفحات ويب خاطئة لمستخدم LobbyAdmin عندما يكون اسم المستخدم مخزنا في قاعدة بيانات RADIUS. يتم تقديم LobbyAdmin بواجهة ReadOnly بدلا من واجهة LobbyAdmin.

تم حل هذا الخطأ في WLC، الإصدار 4.0.206.0. لذلك، تأكد من أن إصدار وحدة التحكم لديك هو 4.0.206.0 أو إصدار أحدث. ارجع إلى [ترقية برنامج وحدة تحكم الشبكة المحلية اللاسلكية \(WLC\)](#) للحصول على تعليمات حول كيفية ترقية وحدة التحكم إلى الإصدار المناسب.

لتنفيذ مصادقة إدارة وحدة التحكم باستخدام خادم RADIUS، تأكد من تمكين علامة Admin-auth-via-RADIUS على وحدة التحكم. يمكن التحقق من هذا من مخرج الأمر `show radius summary`.

تتمثل الخطوة الأولى في تكوين معلومات خادم RADIUS على وحدة التحكم وإنشاء إمكانية الوصول إلى الطبقة 3 بين وحدة التحكم وخادم RADIUS.

### [تكوين معلومات خادم RADIUS على وحدة التحكم](#)

أتمت هذا steps in order to شكلت ال WLC مع تفاصيل حول ال ACS:

1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، أختار علامة التبويب الأمان وقم بتكوين عنوان IP والسر المشترك لخادم ACS. يجب أن يكون هذا السر المشترك هو نفسه على ACS in order for WLC أن يتصل مع ACS. ملاحظة: سر ACS المشترك حساس لحالة الأحرف. لذلك، تأكد من إدخال المعلومات السرية المشتركة بشكل صحيح. يوضح هذا الشكل مثلا:

The screenshot shows the Cisco WLC GUI for configuring a new RADIUS Authentication Server. The 'Management' checkbox is highlighted with a red box. The configuration includes:

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. حدد خانة الاختيار إدارة للسماح ل ACS بإدارة مستخدمي WLC كما هو موضح في الشكل في الخطوة 1. بعد ذلك، انقر فوق تطبيق.
3. تحقق من إمكانية الوصول إلى الطبقة 3 بين وحدة التحكم وخادم RADIUS الذي تم تكوينه باستخدام تعليمات الأمر ping. ويتوفر خيار اختبار الاتصال هذا أيضا على صفحة خادم RADIUS التي تم تكوينها في واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) في علامة التبويب الأمان > مصادقة RADIUS. يوضح هذا الرسم التخطيطي ردا ناجحا على اختبار الاتصال من خادم RADIUS. لذلك، تتوفر إمكانية الوصول إلى الطبقة 3 بين وحدة التحكم وخادم RADIUS.

CISCO

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

Security

AAA

General

RADIUS

Authentication

Accounting

Fallback

TACACS+

LDAP

Local Net Users

MAC Filtering

Disabled Clients

User Login Policies

AP Policies

Password Policies

RADIUS Authentication Servers

Call Station ID Type: IP Address

Use AES Key Wrap:  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	10.78.177.16	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.77.244.197	1812	Disabled	Enabled

## تكوين خادم RADIUS

أكمل الخطوات الواردة في هذه الأقسام لتكوين خادم RADIUS:

1. إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA إلى خادم RADIUS
2. قم بتكوين السمة المناسبة من نوع خدمة RADIUS IETF لمسؤول البهو

## إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA إلى خادم RADIUS

أكمل هذه الخطوات لإضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA في خادم RADIUS. وكما ذكر سابقاً، يستخدم هذا المستند ACS كخادم RADIUS. يمكنك استخدام أي خادم RADIUS لهذا التكوين.

أتمت هذا steps in order to أضفت ال WLC كعميل AAA في ال ACS:

1. من واجهة المستخدم الرسومية (ACS)، اختر علامة التبويب تكوين الشبكة.
2. تحت عملاء AAA، انقر فوق إضافة إدخال.
3. دخلت في الإضافة aaa زبون نافذة، ال WLC مضيف إسم، العنوان من ال WLC، ومفتاح سري مشترك. راجع مخطط المثال ضمن الخطوة 5.
4. من القائمة المنسدلة مصادقة باستخدام، اختر Cisco Aironet (RADIUS).
5. انقر فوق إرسال + إعادة تشغيل لحفظ التكوين.



## Add AAA Client



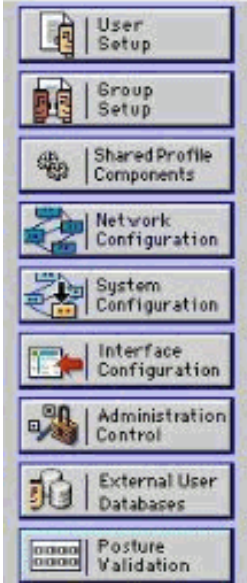
AAA Client Hostname	<input type="text" value="WLC2"/>
AAA Client IP Address	<input type="text" value="10.77.244.212"/>
Shared Secret	<input type="text" value="cisco123"/>
<b>RADIUS Key Wrap</b>	
Key Encryption Key	<input type="text"/>
Message Authenticator Code Key	<input type="text"/>
Key Input Format	<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	

### قم بتكوين السمة المناسبة من نوع خدمة RADIUS IETF لمسؤول الياهو

لمصادقة مستخدم إدارة وحدة تحكم كمسؤول لوحة تحكم عبر خادم RADIUS، يجب إضافة المستخدم إلى قاعدة بيانات RADIUS مع تعيين سمة نوع الخدمة IETF RADIUS إلى **Administrative**. تقوم هذه السمة بتعيين دور المستخدم المحدد لمسؤول يهو على وحدة تحكم.

ييدي هذا وثيقة المثالالمستخدمإدارة اللوبي كمسؤول لوبي. أتمت in order to شكلت هذا مستعمل، هذا steps على ال ACS:

1. من واجهة المستخدم الرسومية (ACS)، أختار علامة التبويب إعداد المستخدم.
2. دخلت ال username أن يكون أضفت إلى ال ACS بما أن هذا مثال ييدي نافذة:



User: 
Find Add/Edit

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

List all users

Remove Dynamic Users

3. انقر فوق إضافة/تحرير للانتقال إلى صفحة تحرير المستخدم.
4. في صفحة تحرير المستخدم، قم بتوفير الاسم الحقيقي والوصف وتفاصيل كلمة المرور الخاصة بهذا المستخدم. في هذا مثال، ال username وكلمة يستعمل على حد سواء اللوبي Admin.

## User: lobbyadmin (New User)

 Account Disabled

Supplementary User Info <span style="float: right;">?</span>	
Real Name	<input type="text" value="Lobby Admin"/>
Description	<input type="text" value="Lobby Admin"/>

User Setup <span style="float: right;">?</span>	
<b>Password Authentication:</b>	
	<input type="text" value="ACS Internal Database"/>
CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)	
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>
<input type="checkbox"/> Separate (CHAP/MS-CHAP/ARAP)	
Password	<input type="text"/>
Confirm Password	<input type="text"/>
<small>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 cards are enabled.</small>	
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

5. قم بالتمرير لأسفل إلى إعداد سمات IETF RADIUS وحدد خانة الاختيار **سمة نوع الخدمة**.
6. أختار إدارة رد الاتصال من القائمة المنسدلة نوع الخدمة وانقر فوق إرسال. هذه هي السمة التي تعين لهذا المستخدم دور مسؤول البهو.



## 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:

Failed attempts exceed:

Failed attempts since last successful login: 0

Reset current failed attempts count on submit

### IETF RADIUS Attributes

[006] Service-Type

في بعض الأحيان، لا تكون سمة "نوع الخدمة" هذه مرئية ضمن إعدادات المستخدم. في مثل هذه الحالات، أكمل الخطوات التالية من أجل جعلها مرئية: من واجهة المستخدم الرسومية (ACS)، اختر **تكوين الواجهة < RADIUS (IETF** لتمكين سمات IETF في نافذة تكوين المستخدم. وهذا ينقلك إلى صفحة إعدادات RADIUS (IETF). من صفحة إعدادات RADIUS (IETF)، يمكنك تمكين سمة IETF التي يجب أن تكون مرئية تحت إعدادات المستخدم أو المجموعة. بالنسبة لهذا التكوين، تحقق من **نوع الخدمة** لعمود المستخدم وانقر فوق إرسال. يوضح هذا الإطار مثالاً:



## RADIUS (IETF)

- 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	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

**ملاحظة:** يحدد هذا المثال المصادقة على أساس كل مستخدم. يمكنك أيضا إجراء المصادقة استنادا إلى المجموعة التي ينتمي إليها مستخدم معين. في مثل هذه الحالات، حدد خانة الاختيار **مجموعة** بحيث تكون هذه السمة مرئية تحت إعدادات المجموعة. **ملاحظة:** أيضا، إذا كانت المصادقة على أساس المجموعة، فأنت بحاجة إلى تعيين مستخدمين إلى مجموعة معينة وتكوين سمات IETF لإعداد المجموعة لتوفير امتيازات الوصول لمستخدمي تلك المجموعة. ارجع إلى **إدارة مجموعة المستخدمين** للحصول على معلومات تفصيلية حول كيفية تكوين المجموعات وإدارتها.

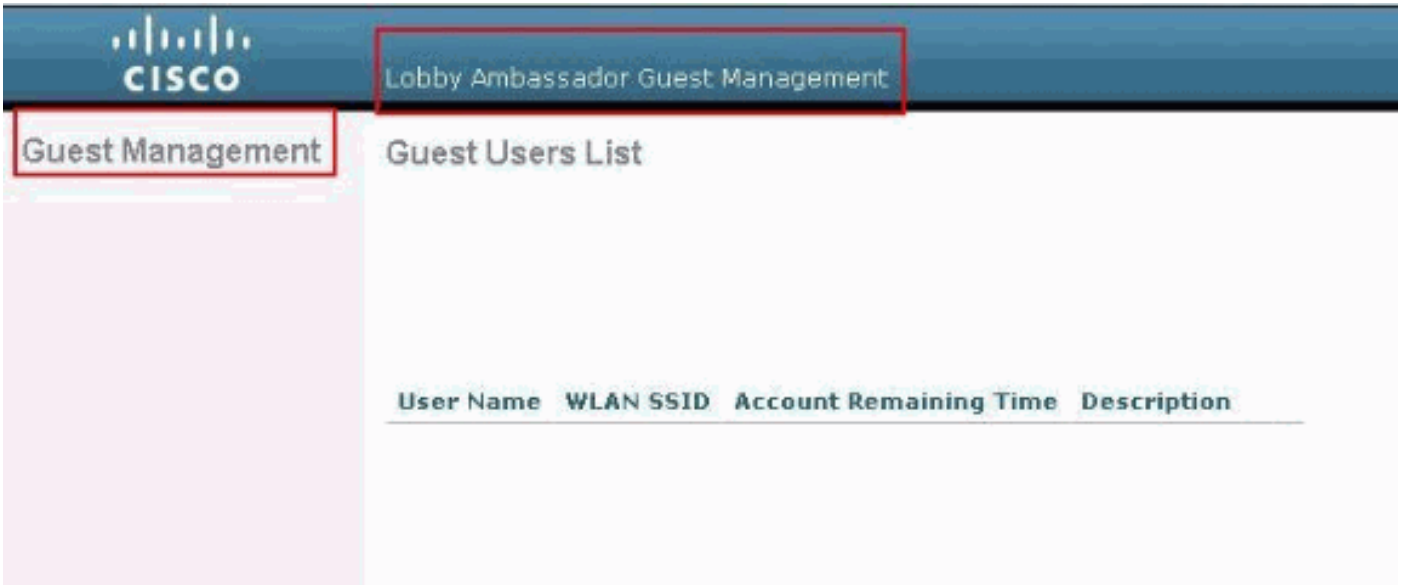
## [التحقق من الصحة](#)

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

للتحقق من أن التكوين لديك يعمل بشكل صحيح، قم بالوصول إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من خلال وضع واجهة المستخدم الرسومية (HTTP/HTTPS) (GUI).

**ملاحظة:** لا يمكن لسفير بهو الوصول إلى واجهة واجهة سطر الأوامر الخاصة بوحدة التحكم، وبالتالي يمكنه إنشاء حسابات مستخدمين زائرين فقط من واجهة المستخدم الرسومية (GUI) لوحدة التحكم.

عندما تظهر مطالبة تسجيل الدخول، أدخل اسم المستخدم وكلمة المرور كما تم تكوينهما على ACS. إذا كانت التكوينات لديك صحيحة، فإنه تتم مصادقتك بنجاح في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كمسؤول بساحة انتظار. يوضح هذا المثال كيفية ظهور واجهة المستخدم الرسومية (GUI) لمسؤول البهو بعد المصادقة الناجحة:



**ملاحظة:** يمكنك أن ترى أن مسؤول البهو ليس لديه خيار آخر بخلاف إدارة المستخدم الضيف.

للتحقق من ذلك من وضع CLI، يدخل Telnet في وحدة التحكم كمسؤول للقراءة والكتابة. قم بإصدار الأمر `debug aaa all enable` في واجهة سطر الأوامر (CLI) لوحدة التحكم.

```

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
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*
      .....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 09 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
CACS:0/ae26/a4.. 34
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*

```

في المعلومات المبرزة في هذا الإخراج، يمكنك أن ترى أن السمة 11 لنوع الخدمة (CallBack Administrative) تم تمريرها إلى وحدة التحكم من خادم ACS وأن المستخدم سجل الدخول كمسؤول باللوحة.

قد تكون هذه الأوامر ذات فائدة إضافية:

- تمكين تفاصيل debug aaa
- debug aaa events enable
- debug aaa packet enable

ملاحظة: ارجع إلى [معلومات مهمة حول أوامر التصحيح](#) قبل استخدام أوامر debug.

## استكشاف الأخطاء وإصلاحها

عند تسجيل الدخول إلى وحدة تحكم ذات امتيازات سفير مجموعة الضغط، لا يمكنك إنشاء حساب مستخدم ضيف بقيمة مدة البقاء "0"، وهو حساب لا ينتهي أبداً. في هذه الحالات، تستلم Lifetime 0 رسالة خطأ.

هذا إلى cisco بق CSCsf32392 id (يسجل زبون فقط)، أي يكون أساساً مع WLC صيغة 4.0. تم حل هذا الخطأ في WLC، الإصدار 4.1.

## معلومات ذات صلة

- [مصادقة خادم RADIUS لمستخدمي الإدارة على مثال تكوين وحدة التحكم](#)
- [تكوين TACACS+ للشبكة اللاسلكية الموحدة من Cisco](#)
- [دليل تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco، الإصدار 4.0 - إدارة حسابات المستخدم](#)
- [مثال على تكوين ACL على وحدة تحكم الشبكة المحلية اللاسلكية](#)
- [الأسئلة المتداولة حول وحدة التحكم في الشبكة المحلية اللاسلكية \(WLC\)](#)

- قوائم التحكم في الوصول على وحدات التحكم في الشبكة المحلية اللاسلكية: القواعد والحدود والأمثلة
- مثال تكوين المصادقة الخارجية للويب مع وحدات تحكم الشبكة المحلية (LAN) اللاسلكية
- مثال تكوين مصادقة الويب لوحدة تحكم الشبكة المحلية (LAN) اللاسلكية
- Guest WLAN و WLAN الداخلية باستخدام مثال تكوين WLCs
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا اذ ه Cisco ت مچرت  
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا