

# مكحتلا تادحو مادختساب EAP ةقداصم نيوكت (WLC) ةيكلساللا ةيلحمللا ةكبشللا يف

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) للتشغيل الأساسي وتسجيل نقاط الوصول في الوضع Lightweight إلى وحدة التحكم](#)

[تكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) لمصادقة RADIUS من خلال خادم RADIUS خارجي](#)

[تكوين معلمات WLAN](#)

[قم بتكوين ACS الآمن من Cisco كخادم RADIUS خارجي وقم بإنشاء قاعدة بيانات مستخدم لعملاء المصادقة](#)

[تكوين العميل](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[تلميحات استكشاف المشكلات وإصلاحها](#)

[التعامل مع مؤقتات EAP](#)

[إستخراج ملف الحزمة من خادم ACS RADIUS لاستكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## المقدمة

يشرح هذا المستند كيفية تكوين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة بروتوكول المصادقة المتوسع (EAP) باستخدام خادم RADIUS خارجي. يستخدم مثال التكوين هذا خادم التحكم في الوصول الآمن (ACS) من Cisco كخادم RADIUS الخارجي للتحقق من مسوغات المستخدم.

## المتطلبات الأساسية

### المتطلبات

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

- معرفة أساسية بتكوين نقاط الوصول في الوضع (APs) Lightweight و Cisco WLCs.
- معرفة أساسية ببروتوكول نقطة الوصول في الوضع (LWAPP) Lightweight.
- معرفة كيفية تكوين خادم RADIUS خارجي مثل Cisco Secure ACS.

## المكونات المستخدمة

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

- نقطة الوصول في الوضع Lightweight من سلسلة Cisco Aironet 1232AG
  - Cisco 4400 Series WLC الذي يشغل البرنامج الثابت 5.1
  - Cisco Secure ACS الذي يشغل الإصدار 4.1
  - مهائى عميل Cisco Aironet 802.11 a/b/g
  - أداة (Cisco Aironet Desktop Utility (ADU) التي تشغل البرنامج الثابت 4.2
- 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 تلمحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

## التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

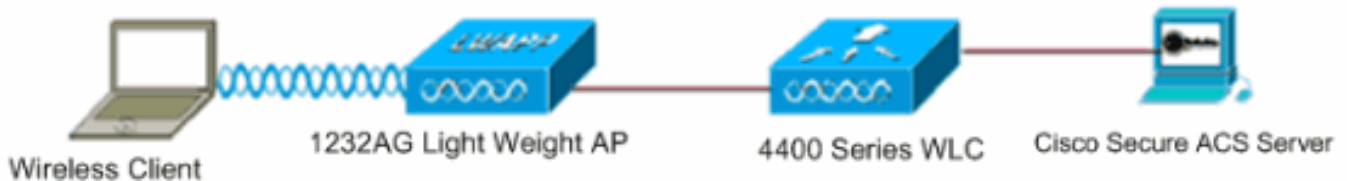
**ملاحظة:** أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

أكمل هذه الخطوات لتكوين الأجهزة لمصادقة EAP:

1. [قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) للتشغيل الأساسي وتسجيل نقاط الوصول في الوضع Lightweight إلى وحدة التحكم.](#)
2. [قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) لمصادقة RADIUS من خلال خادم RADIUS خارجي.](#)
3. [قم بتكوين معلمات WLAN.](#)
4. [قم بتكوين ACS الآمن من Cisco كخادم RADIUS خارجي وقم بإنشاء قاعدة بيانات مستخدم لمصادقة العملاء.](#)

## الرسم التخطيطي للشبكة

في هذا الإعداد، يتم توصيل Cisco 4400 WLC ونقطة وصول في الوضع Lightweight من خلال موزع. كما يتم توصيل خادم RADIUS الخارجي (Cisco Secure ACS) بنفس الموزع. توجد جميع الأجهزة في الشبكة الفرعية نفسها. يتم تسجيل نقطة الوصول في البداية إلى وحدة التحكم. يجب تكوين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) ونقطة الوصول (AP) لمصادقة بروتوكول المصادقة المتوسع (LEAP) في الوضع Lightweight. يستخدم العملاء المتصلون بنقطة الوصول مصادقة LEAP من أجل الاقتران بنقطة الوصول. يتم استخدام مصدر المحتوى الإضافي الآمن من Cisco لإجراء مصادقة RADIUS.



## قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للتشغيل الأساسي وتسجيل نقاط الوصول في الوضع Lightweight إلى وحدة التحكم

أستخدم معالج تكوين بدء التشغيل على واجهة سطر الأوامر (CLI) لتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية. بدلا من ذلك، يمكنك أيضا استخدام واجهة المستخدم الرسومية (GUI) لتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يشرح هذا المستند التكوين على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) باستخدام معالج تكوين بدء التشغيل على واجهة سطر الأوامر.

بعد تمهيد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لأول مرة، يدخل مباشرة في معالج تكوين بدء التشغيل. أستخدم معالج التكوين لتكوين الإعدادات الأساسية. يمكنك تشغيل المعالج على CLI أو واجهة المستخدم الرسومية. يوضح هذا الإخراج مثلا لمعالج تكوين بدء التشغيل على CLI (واجهة سطر الأوامر):

```
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

تقوم هذه المعلمات بإعداد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية. في مثال التكوين هذا، يستخدم عنصر التحكم في الشبكة المحلية اللاسلكية (10.77.244.204) عنوان IP لواجهة الإدارة و10.77.244.205 عنوان IP لواجهة AP-Manager.

قبل تكوين أي ميزات أخرى على قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs)، يجب على نقاط الوصول في الوضع Lightweight التسجيل مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يفترض هذا المستند أن نقطة الوصول في الوضع Lightweight مسجلة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). أحلت [الخفيف](#) وزن [ap \(ثني\) تسجيل إلى لاسلكي lan جهاز تحكم \(WLC\)](#) ل كثير معلومة على كيف الخفيف وزن APs يسجل مع ال WLC.

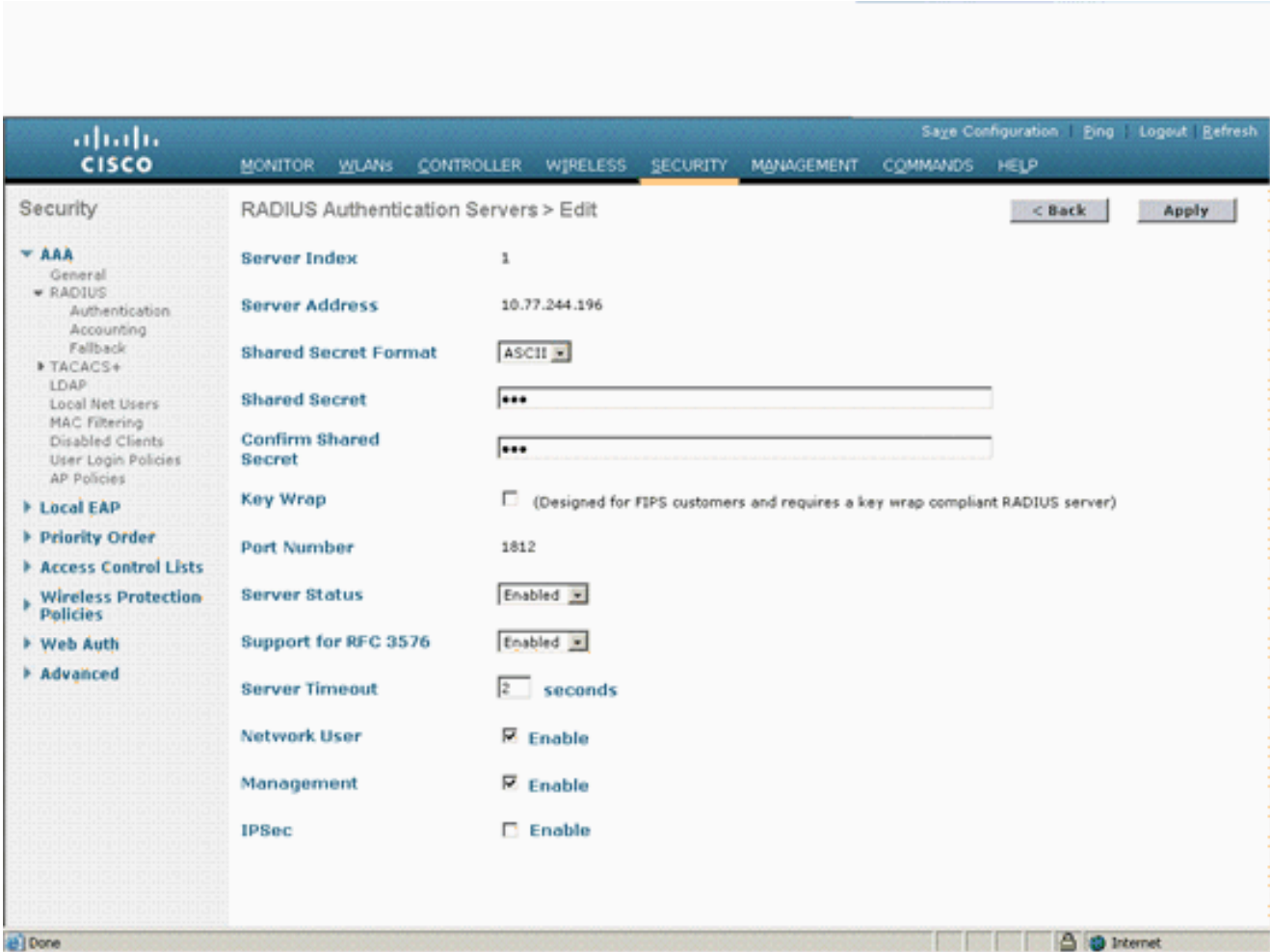
## تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة RADIUS من خلال خادم RADIUS خارجي

يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم

RADIUS خارجي. ثم يتحقق خادم RADIUS الخارجي من مسوغات المستخدم ويوفر الوصول إلى العملاء اللاسلكيين.

أتمت هذا steps in order to شكلت ال WLC لخادم خارجي RADIUS:

1. أختار تأمين ومصادقة RADIUS من واجهة المستخدم الرسومية (GUI) لوحدة التحكم لعرض صفحة خوادم مصادقة RADIUS. ثم انقر فوق جديد لتحديد خادم RADIUS.



2. قم بتعريف معلمات خادم RADIUS في خوادم مصادقة RADIUS < صفحة جديدة. وتتضمن هذه المعلمات عنوان IP لخادم RADIUS والسر المشترك ورقم المنفذ وحالة الخادم. تحدد خانة الاختيار لمستخدم الشبكة وإدارتها ما إذا كانت المصادقة المستندة إلى RADIUS تنطبق على إدارة WLC ومستخدمي الشبكة. يستعمل هذا مثال ال cisco يأمن ACS كخادم RADIUS مع عنوان 10.77.244.196.
3. يمكن الآن استخدام خادم RADIUS بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للمصادقة. يمكنك العثور على خادم RADIUS المسرود إذا أخترت التأمين < RADIUS < المصادقة.

Security

AAA

- General
- RADIUS
  - Authentication
  - Accounting
  - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering

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)

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

يتم دعم RFC 3576 على خادم RADIUS Cisco CNS Access Registrar (CAR)، ولكن ليس على خادم ACS من الإصدار 4.0 والإصدارات الأقدم. كما يمكنك استخدام ميزة خادم RADIUS المحلي لمصادقة المستخدمين. تم تقديم خادم RADIUS المحلي مع رمز الإصدار 4.1.171.0. لا تحتوي قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs) التي تشغل الإصدارات السابقة على ميزة RADIUS المحلية. EAP المحلي هو أسلوب مصادقة يسمح للمستخدمين والعملاء اللاسلكيين بالمصادقة محلياً. وقد تم تصميمه للاستخدام في المكاتب البعيدة التي ترغب في الحفاظ على الاتصال بالعملاء اللاسلكيين عند تعطل النظام الخلفي أو تعطل خادم المصادقة الخارجي. يسترجع EAP المحلي مسوغات المستخدم من قاعدة بيانات المستخدم المحلية أو قاعدة بيانات خلفية LDAP لمصادقة المستخدمين. يدعم EAP المحلي المصادقة على LEAP و EAP-FAST مع مسوغات الوصول المحمي PAC و EAP-FAST مع الشهادات و EAP-TLS بين وحدة التحكم والعملاء اللاسلكيين. يتم تصميم EAP المحلي كنظام لمصادقة النسخ الاحتياطي. في حالة تكوين أي خوادم RADIUS على وحدة التحكم، تحاول وحدة التحكم مصادقة العملاء اللاسلكيين باستخدام خوادم RADIUS أولاً. لا يتم محاولة EAP المحلي إلا في حالة عدم العثور على خوادم RADIUS، إما بسبب انتهاء مهلة خوادم RADIUS أو بسبب عدم تكوين خوادم RADIUS. راجع [مصادقة EAP المحلية على وحدة تحكم الشبكة المحلية اللاسلكية باستخدام EAP-FAST ومثال تكوين خادم LDAP](#) للحصول على مزيد من المعلومات حول كيفية تكوين EAP المحلي على وحدات تحكم الشبكة المحلية اللاسلكية.

## تكوين معلمات WLAN

بعد ذلك، قم بتكوين شبكة WLAN التي يستخدمها العملاء للاتصال بالشبكة اللاسلكية. عندما قمت بتكوين المعلمات الأساسية لـ WLC، قمت أيضاً بتكوين SSID لـ WLAN. يمكنك استخدام SSID هذا للشبكة المحلية اللاسلكية (WLAN) أو إنشاء SSID جديد. في هذا المثال، يمكنك إنشاء SSID جديد.

**ملاحظة:** يمكنك تكوين ما يصل إلى ستة عشر شبكة WLAN على وحدة التحكم. يمكن أن يتحكم حل Cisco WLAN في ما يصل إلى ستة عشر شبكة WLAN لنقاط الوصول في الوضع Lightweight. يمكن تعيين نهج أمان فريدة لكل شبكة محلية لاسلكية. تقوم نقاط الوصول في الوضع Lightweight بث جميع شبكات WLAN الخاصة بحل Cisco WLAN النشط وفرض السياسات التي تحددها لكل شبكة محلية لاسلكية (WLAN).

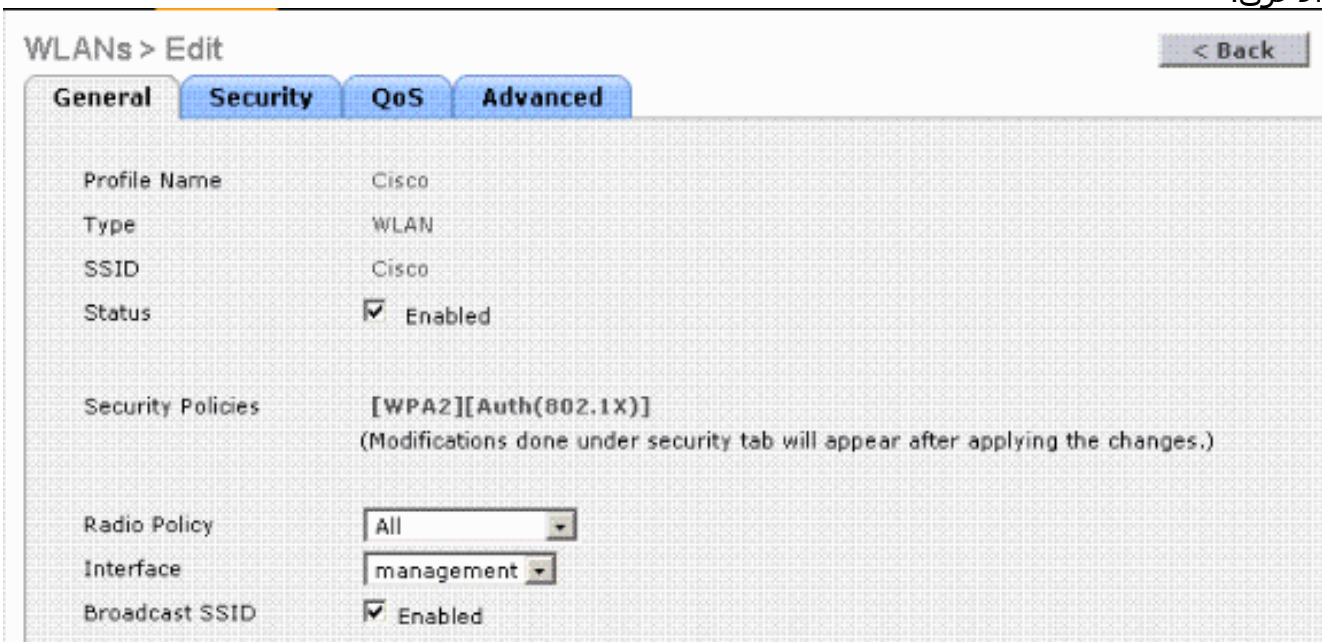
أكمل الخطوات التالية لتكوين شبكة WLAN جديدة والمعلمات المرتبطة بها:

1. طقطقت WLANs من ال gui من الجهاز تحكم in order to عرضت WLANs صفحة. تسرد هذه الصفحة شبكات WLAN الموجودة على وحدة التحكم.
2. أشرت جديد in order to خلقت WLAN جديد. أدخل اسم التوصيف واسم الشبكة المحلية اللاسلكية (WLAN) للشبكة المحلية اللاسلكية (WLAN) ثم انقر على تطبيق. يستخدم هذا المثال Cisco كـ معرف SSID.



The image shows the Cisco WLAN configuration interface for creating a new WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > New' and contains three fields: 'Type' set to 'WLAN', 'Profile Name' set to 'Cisco', and 'WLAN SSID' set to 'Cisco'.

3. ما إن يخلق أنت WLAN جديد، ال WLAN < تحرير صفحة ل ال WLAN جديد يظهر. في هذه الصفحة، يمكنك تحديد معلمات مختلفة خاصة بشبكة WLAN هذه تتضمن السياسات العامة ونهج الأمان ونهج جودة الخدمة والمعلومات المتقدمة الأخرى.



The image shows the Cisco WLAN configuration interface for editing an existing WLAN. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', and 'MANAGEMENT'. The left sidebar shows 'WLANs' with sub-items 'WLANs' and 'Advanced'. The main content area is titled 'WLANs > Edit' and contains a 'Back' button. Below the title are four tabs: 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is selected and shows the following configuration: Profile Name: Cisco, Type: WLAN, SSID: Cisco, Status:  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:  Enabled.

أختر الواجهة المناسبة من القائمة المنسدلة. يمكن تعديل المعلومات الأخرى استنادا إلى متطلبات شبكة WLAN. حدد مربع الحالة ضمن السياسات العامة لتمكين شبكة WLAN. انقر صفحة التأمين واختر تأمين الطبقة 2. من القائمة المنسدلة تأمين الطبقة 2، اختر 802.1x. في معاملات 802.1x، اختر حجم مفتاح WEP. يستخدم هذا المثال مفتاح WEP 128-بت، وهو مفتاح WEP 104-بت بالإضافة إلى متجه تهيئة 24-بت.

## WLANs > Edit

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Layer 2 Security: 802.1X  
 MAC Filtering

**802.1X Parameters**

802.11 Data Encryption	Type	Key Size
<input checked="" type="radio"/>	WEP	104 bits

5. أختار علامة التويب خوادم AAA. من القائمة المنسدلة لخوادم المصادقة (RADIUS)، أختار خادم RADIUS المناسب. يستخدم هذا الخادم لمصادقة العملاء اللاسلكيين.

## WLANs > Edit

**General** **Security** **QoS** **Advanced**

**Layer 2** **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

Radius Servers		LDAP Servers	
Authentication Servers	Accounting Servers	Server 1	Server 2
	<input checked="" type="checkbox"/> Enabled	Server 1	Server 2
Server 1	IP:10.77.244.196, Port:1812	None	None
Server 2	None	None	None
Server 3	None	None	None

**Local EAP Authentication**

Local EAP Authentication  Enabled

6. قطعة يطبق in order to أنقذت التشكيل.

## قم بتكوين ACS الأمن من Cisco كخادم RADIUS خارجي وقم بإنشاء قاعدة بيانات مستخدم لعملاء المصادقة

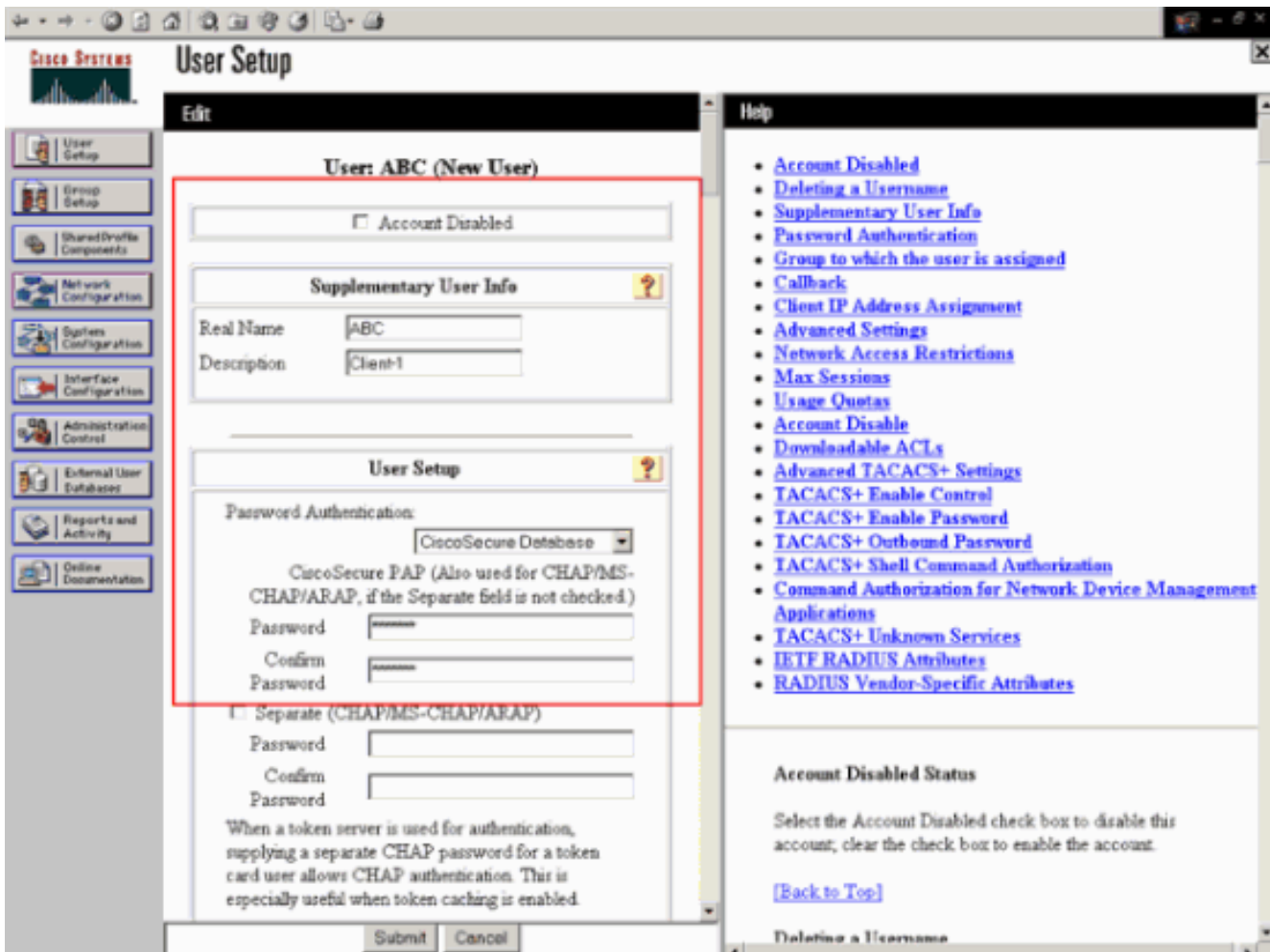
أكمل الخطوات التالية لإنشاء قاعدة بيانات المستخدم وتمكين مصادقة EAP على مصدر المحتوى الإضافي الأمن من Cisco:

1. أختارت مستعمل setup من ال ACS gui، دخلت ال username، و قطعة يضيف/يحرر. في هذا المثال، المستخدم هو .ABC

The screenshot shows the Cisco User Setup web interface. On the left, there is a sidebar with navigation options: User Setup, Group Setup, Shared/Write Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is split into two panes. The left pane, titled 'Select', contains a search box with 'User: ABC' entered, a 'Find' button, and an 'Add/Edit' button. Below the search box is a grid of letters (A-Z) and a 'List All Users' button. The right pane, titled 'Help', contains a list of links for user management and a detailed explanation of the 'User Setup and External User Databases' section, including a note about configuration overrides and a warning about the Unknown User Policy.

2. عندما تظهر صفحة إعداد المستخدم، قم بتعريف كافة المعلمات الخاصة بالمستخدم. في هذا المثال، يتم تكوين اسم المستخدم وكلمة المرور ومعلومات المستخدم التكميلية لأنك بحاجة فقط إلى هذه المعلمات لمصادقة EAP. انقر فوق إرسال وتكرار نفس العملية لإضافة المزيد من المستخدمين إلى قاعدة البيانات. بشكل افتراضي يتم تجميع كافة المستخدمين تحت المجموعة الافتراضية ويتم تعيين نفس النهج كما هو محدد للمجموعة. راجع [قسم إدارة مجموعة المستخدمين في دليل المستخدم ل Cisco Secure ACS ل Windows Server 3.2](#) للحصول على مزيد من المعلومات إذا كنت تريد تعيين مستخدمين محددتين إلى مجموعات مختلفة.



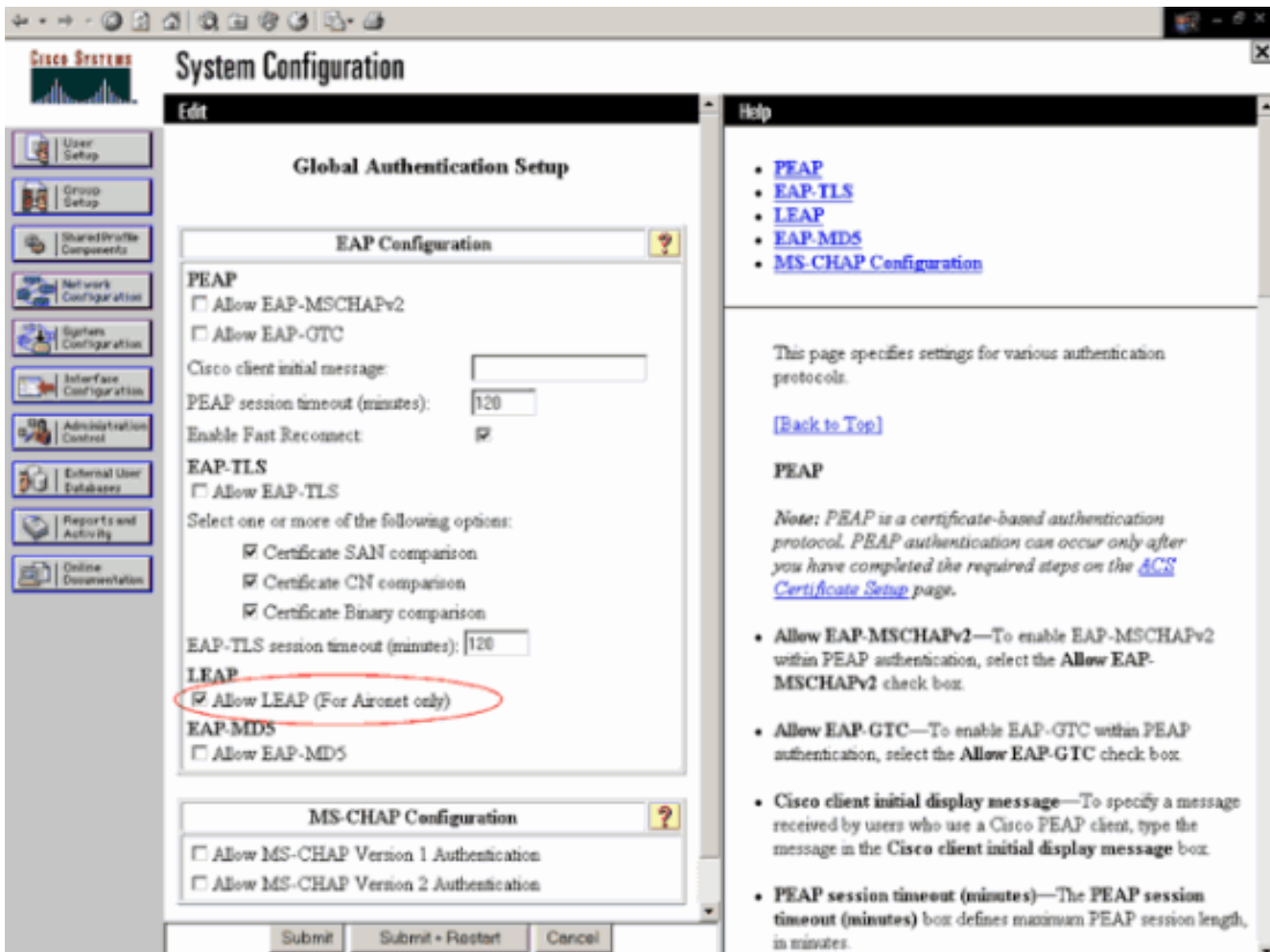


3. قم بتعريف وحدة التحكم كعميل AAA على خادم ACS. طقطقت شبكة تشكيل من ال ACS gui عندما تظهر صفحة تكوين الشبكة، قم بتعريف اسم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وعنوان بروتوكول الإنترنت (IP) والسر المشترك وطريقة المصادقة (RADIUS Cisco Airespace). ارجع إلى الوثائق من الشركة المصنعة الخاصة بخوادم المصادقة الأخرى غير الخاصة ب ACS. ملاحظة: يجب أن يتطابق المفتاح السري المشترك الذي تقوم بتكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وخادم ACS. السر المشترك حساس لحالة الأحرف.

## 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/>	
<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
<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. انقر على تكوين النظام وإعداد المصادقة العامة لضمان تكوين خادم المصادقة لتنفيذ أسلوب مصادقة EAP المطلوب. تحت إعدادات تكوين EAP، اختر أسلوب EAP المناسب. يستخدم هذا المثال مصادقة LEAP. انقر فوق إرسال عند الانتهاء.



## تكوين العميل

كما يجب تكوين العميل وفق نوع EAP المناسب. يقترح العميل نوع EAP على الخادم أثناء عملية تفاوض EAP. إذا كان الخادم يدعم هذا النوع من نقاط الوصول EAP، فإنه يعترف بنوع EAP. إذا لم يكن نوع EAP مدعوماً، يرسل إقراراً سلبياً ويتفاوض العميل مرة أخرى مع أسلوب EAP مختلف. وتستمر هذه العملية حتى يتم التفاوض على نوع EAP معتمد. يستخدم هذا المثال LEAP كنوع EAP.

أكمل هذه الخطوات لتكوين LEAP على العميل باستخدام أداة Aironet Desktop Utility .

1. انقر نقرًا مزدوجًا على رمز الأداة المساعدة Aironet لفتحه.
2. انقر على علامة تبويب إدارة التوصيفات.
3. انقر على ملف تخصيص واختر تعديلاً.
4. تحت علامة التبويب عام، اختر اسم ملف تخصيص. أدخل SSID للشبكة المحلية اللاسلكية.

Profile Management

General Security Advanced

Profile Settings

Profile Name: Cisco123

Client Name: WIRELESS123

Network Names

SSID1: cisco

SSID2:

SSID3:

OK Cancel

ملا (WLAN).

حظة: يعد SSID متحسسا لحالة الأحرف ويجب مطابقته تماما مع SSID المكون على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

5. تحت علامة التبويب أمان، أختَر 802.1x. أختَر نوع EAP على هيئة LEAP وانقر

Profile Management

General Security Advanced

Set Security Options

WPA/WPA2/CCKM WPA/WPA2/CCKM EAP Type: LEAP

WPA/WPA2 Passphrase

802.1x 802.1x EAP Type: LEAP

Pre-Shared Key (Static WEP)

None

Configure...

Allow Association to Mixed Cells

Profile Locked

Limit Time for Finding Domain Controller To: 0 sec

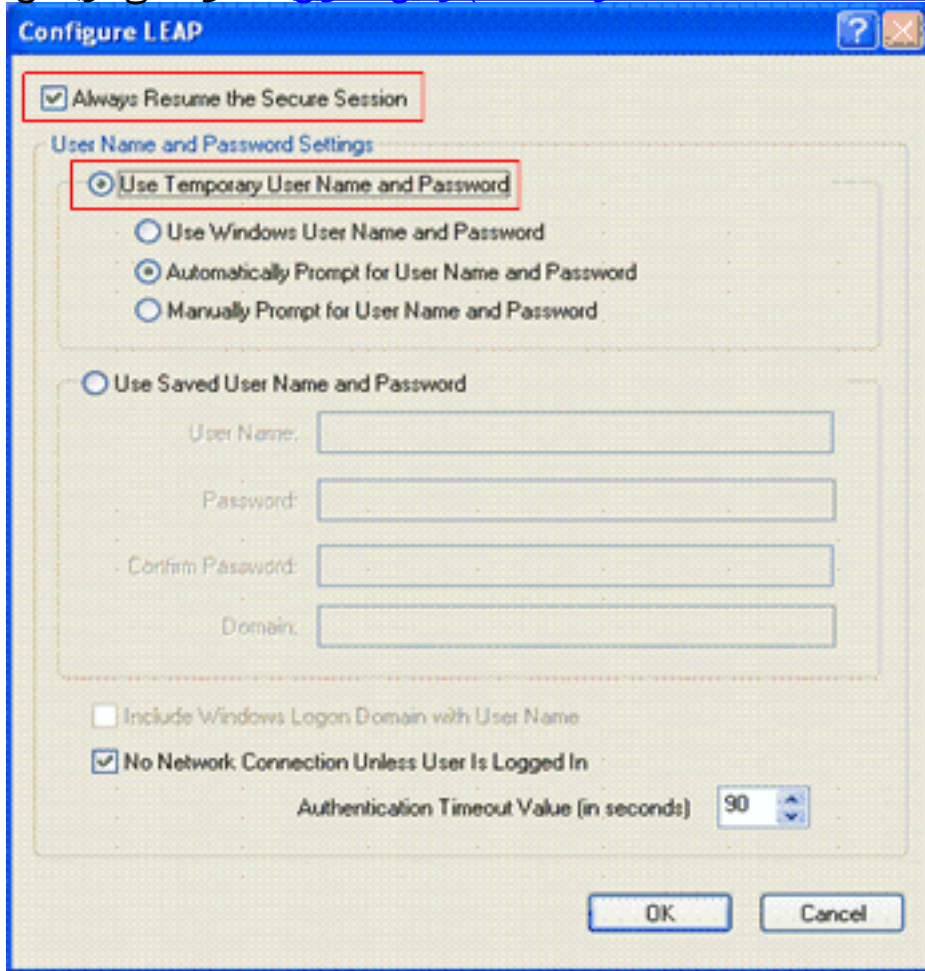
Group Policy Delay: 60 sec

OK Cancel

تكوين.

6. أختَر استخدام اسم المستخدم المؤقت وكلمة المرور، والذي يطلب منك إدخال بيانات المستخدم في كل مرة يتم فيها إعادة تمهيد الكمبيوتر. تحقق من أحد الخيارات الثلاثة المتوفرة هنا. يستخدم هذا المثال المطالبة تلقائيا باسم المستخدم وكلمة المرور، والذي يتطلب منك إدخال بيانات اعتماد مستخدم LEAP بالإضافة إلى اسم مستخدم وكلمة مرور Windows قبل تسجيل الدخول إلى Windows. حدد خانة الاختيار إستئناف جلسات العمل

الآمنة دائما" الموجودة في أعلى النافذة إذا كنت تريد من متلقي LEAP أن يحاول دائما إستئناف جلسة العمل السابقة دون الحاجة إلى مطالبتك بإعادة إدخال بيانات الاعتماد كلما تجول محول العميل على الشبكة أو قام بإعادة تعيينه. ملاحظة: ارجع إلى قسم [تكوين مهائى العميل](#) في المستند [مهايات عميل شبكة LAN اللاسلكية](#) (CB21AG و Cisco Aironet 802.11a/b/g و PI21AG) [ودليل التكوين](#) للحصول على مزيد من المعلومات حول



الخيارات الأخرى.

7. تحت علامة التبويب **خيارات متقدمة**، يمكنك تكوين التمهيدي وامتداد Aironet وخيارات 802.11 الأخرى مثل الطاقة والتردد وما إلى ذلك.
8. وانقر فوق OK. يحاول العميل الآن الاقتران بالمعلومات التي تم تكوينها.

## التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

حاول إقران عميل لاسلكي بنقطة الوصول في الوضع Lightweight باستخدام مصادقة LEAP للتحقق من عمل التكوين كما هو متوقع.

**ملاحظة:** يفترض هذا المستند تكوين ملف تعريف العميل لمصادقة LEAP. ارجع إلى [إستخدام مصادقة EAP](#) للحصول على مزيد من المعلومات حول كيفية تكوين مهائى العميل اللاسلكي 802.11 a/b/g لمصادقة LEAP.

بمجرد تنشيط توصيف العميل اللاسلكي يطلب من المستخدم توفير اسم المستخدم/كلمة المرور لمصادقة LEAP. فيما يلي مثال:

**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

تمرر نقطة الوصول في الوضع Lightweight ثم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بيانات اعتماد المستخدم إلى خادم RADIUS الخارجي (Cisco Secure ACS) للتحقق من بيانات الاعتماد. يقارن خادم RADIUS البيانات بقاعدة بيانات المستخدم ويوفر الوصول إلى العميل اللاسلكي كلما كانت مسوغات المستخدم صالحة للتحقق من مسوغات المستخدم. يظهر تقرير المصادقة الذي تم تمريره على خادم ACS أن العميل قد اجتاز مصادقة RADIUS. فيما يلي مثال:

The screenshot shows the Cisco Systems Reports and Activity page. The left sidebar contains various configuration and monitoring tools. The main content area displays a table titled "Passed Authentications active.csv" with 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

بعد مصادقة RADIUS الناجحة، يرتبط العميل اللاسلكي بنقطة الوصول في الوضع Lightweight.

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

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.

هذا يستطيع أيضا كنت فحصت تحت المدرب لسان من WLC GUI. أخترت مدرب < زبون وفحصت ل ال MAC عنوان من الزبون.

Save Configuration Ping Logout Refresh

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Monitor 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	<a href="#">Link</a> <a href="#">Test</a> <a href="#">Disable</a> <a href="#">Radius</a>

## استكشاف الأخطاء وإصلاحها

أكمل الخطوات التالية لاستكشاف أخطاء التكوينات وإصلاحها:

1. استخدم الأمر `debug lwapp events enable` للتحقق من تسجيل نقطة الوصول مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
2. تحقق من تلقي خادم RADIUS لطلب المصادقة من العميل اللاسلكي والتحقق من صحته. تحقق من عنوان NAS-IP والتاريخ والوقت للتحقق مما إذا كان عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) قادرا على الوصول إلى خادم RADIUS. تحقق من المصادقة التي تم تمريرها والمحاولات الفاشلة على خادم ACS للقيام بذلك. وهذه التقارير متاحة في إطار التقارير والأنشطة على خادم ACS. فيما يلي مثال على فشل مصادقة خادم RADIUS:

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

ملاحظة: ارجع إلى الحصول على معلومات الإصدار و AAA تصحيح الأخطاء ل Cisco Secure ACS



[Windows](#) للحصول على معلومات حول كيفية أكتشاف الأخطاء وإصلاحها والحصول على معلومات تصحيح الأخطاء على Cisco Secure ACS.

3. يمكنك أيضا استخدام أوامر تصحيح الأخطاء هذه لاستكشاف أخطاء مصادقة AAA وإصلاحها: `debug aaa all:enable` —يشكل تصحيح أخطاء جميع رسائل `AAA.debug dot1x` ربط `enable` —يمكن ال debug من كل ربط `dot1x`. هنا نموذج للمخرجات من الأمر `debug 802.1x aaa enable`:  
(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*
ac:dd:05:00:40:96
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*
        ..e.2].....#...
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, dot1xcb->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*
        ac:dd:05:00:40:96
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

**ملاحظة:** تم تضمين بعض البنود في إخراج تصحيح الأخطاء بسبب قيود المساحة.

4. راقبت ال log on ال WLC in order to فحصت إن ال radius نادل يستلم المستعمل مسوغات. طقطقة مدرب in order to فحصت ال log من ال WLC GUI. من القائمة الموجودة على الجانب الأيسر، انقر فوق إحصائيات وانقر فوق خادم Radius من قائمة الخيارات. هذا مهم جدا لأنه في بعض الحالات، لا يستقبل خادم RADIUS بيانات اعتماد المستخدم أبدا إذا كان تكوين خادم RADIUS على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) غير صحيح. هذه هي الطريقة التي تظهر بها السجلات على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إذا تم تكوين معلمات RADIUS بشكل غير صحيح:



يمكنك استخدام مجموعة من الأمر **show wlan summary** للتعرف على أي من شبكات WLAN لديك تستخدم مصادقة خادم RADIUS. ثم يمكنك عرض الأمر **show client summary** لترى أي عناوين MAC (العملاء) تمت مصادقتها بنجاح على شبكات WLAN الخاصة ب RADIUS. يمكنك أيضا ربط هذا مع Cisco Secure ACS يمر بمحاولات أو محاولات فاشلة سجل.

## تلميحات استكشاف المشكلات وإصلاحها

- تحقق من أن خادم RADIUS في حالة على وحدة التحكم، وليس على أو .
- استخدم الأمر **ping** للتحقق من إمكانية الوصول إلى خادم Radius من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
- تحقق مما إذا تم تحديد خادم RADIUS من القائمة المنسدلة للشبكة المحلية اللاسلكية (SSID) (WLAN).
- إذا كنت تستخدم WPA، فعليك تثبيت أحدث إصلاح عاجل WPA ل Windows XP SP2. كما يجب عليك ترقية برنامج تشغيل العميل إلى أحدث إصدار.
- إذا قمت بتنفيذ PEAP، على سبيل المثال الشهادات مع XP و SP2 حيث تتم إدارة البطاقات بواسطة الأداة المساعدة Microsoft Wireless-0، تحتاج إلى الحصول على تصحيح KB885453 من Microsoft. إذا كنت تستخدم مسبب Windows Zero Config/client، فقم بتعطيل تمكين إعادة الاتصال السريع. يمكنك تحقيق ذلك إذا اخترت خصائص توصيل الشبكة اللاسلكية < الشبكات اللاسلكية < الشبكات المفضلة. ثم اختر SSID < خصائص < فتح < WEP < مصادقة < نوع PEAP > EAP > خصائص < تمكين إعادة الاتصال السريع . يمكنك بعد ذلك العثور على الخيار لتمكين أو تعطيل في نهاية النافذة.
- إذا كانت لديك بطاقات Intel 2200 أو 2915، فارجع إلى البيانات الموجودة على موقع الويب الخاص بشركة Intel حول المشكلات المعروفة التي تتعلق ببطاقتها: [الاتصال بشبكة الاتصال PRO/Wireless 2200BG من](http://www.intel.com/PRO/Wireless/2200BG) [الاتصال بشبكة الاتصال PRO/Wireless 2915ABG من Intel](http://www.intel.com/PRO/Wireless/2915ABG) قم بتنزيل أحدث برامج التشغيل من Intel لتجنب أي مشكلات. يمكنك تنزيل برامج تشغيل Intel على موقع <http://downloadcenter.intel.com>
- إذا تم تمكين ميزة تجاوز الفشل القوية في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يكون عدائيا للغاية لوضع علامة على خادم AAA على أنه . ولكن، لا ينبغي القيام بذلك لأنه من المحتمل أن لا يستجيب خادم AAA لذلك العميل المعين فقط، إذا قمت بالتجاهل

الصامت. يمكن أن يكون إستجابة لعملاء آخرين صحيحين بشهادات صالحة. ولكن، لا يزال بإمكان عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تمييز خادم AAA على أنه وأنه .للتغلب على هذا الأمر، قم بتعطيل ميزة تجاوز الفشل القوية. قم بإصدار الأمر `config radius aggressive-failover disable` من واجهة المستخدم الرسومية (GUI) لوحدة التحكم لتنفيذ هذا. في حالة تعطيل هذا الإجراء، يفشل وحدة التحكم فقط في الوصول إلى خادم AAA التالي إذا كان هناك ثلاثة عملاء متتاليين يخفون في تلقي إستجابة من خادم .RADIUS

## التعامل مع مؤقتات EAP

أثناء مصادقة 802.1x، قد يرى المستخدم رسالة الخطأ `DOT1X-1-MAX_EAPOL_KEY_RETRANS_FOR_MOBILE: MAX` لرسالة الخطأ `EAPOL-Key M1` `.xx:xx:xx:xx:xx:xx`

تشير رسائل الخطأ هذه إلى أن العميل لم يستجب في الوقت المناسب لوحدة التحكم أثناء تفاوض مفتاح WPA (802.1x). يقوم جهاز التحكم بتعيين مؤقت للاستجابة أثناء التفاوض الأساسي. بشكل نموذجي، عندما ترى هذه الرسالة، فإنه يرجع إلى وجود مشكلة مع الطالب. تأكد من تشغيل أحدث إصدارات برامج تشغيل العملاء والبرامج الثابتة. على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، يوجد عدد قليل من وحدات توقيت EAP التي يمكنك معالجتها للمساعدة في مصادقة العميل. تتضمن مؤقتات EAP هذه:

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

قبل أن تتمكن من معالجة هذه القيم، تحتاج إلى فهم ما تقوم به، وكيف سيؤثر تغييرها على الشبكة:

- **مهلة EAP-IDENTITY-REQUEST:** يؤثر هذا المؤقت على طول فترة الانتظار بين طلبات هوية EAP. بشكل افتراضي، هذه ثانية واحدة (4.1 وأقل) و 30 ثانية (4.2 وأكبر). والسبب في هذا التغيير هو أن بعض العملاء، والخوذة اليدوية، والهواتف، والمساحات الضوئية وما إلى ذلك، واجهوا صعوبة في الاستجابة بالسرعة الكافية. أجهزة مثل الحواسيب المحمولة، عادة لا تتطلب التعامل مع هذه القيم. القيمة المتاحة هي من 1 إلى 120. إذا، ماذا يحدث عندما يتم تعيين هذه السمة على قيمة 30؟ عندما يتصل العميل لأول مرة، فإنه يرسل بداية EAPOL إلى الشبكة، ويرسل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) حزمة EAP، طالبا هوية المستخدم أو الجهاز. إذا لم يستلم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إستجابة الهوية، فإنه يرسل طلب هوية آخر بعد 30 ثانية من الأول. يحدث هذا عند التوصل الأولي، وعندما يجول العميل. ماذا يحدث عندما تزيد هذا المؤقت؟ إذا كان كل شيء على ما يرام، فلن يكون هناك تأثير. ومع ذلك، إذا كانت هناك مشكلة في الشبكة (بما في ذلك مشاكل العملاء أو مشاكل نقطة الوصول أو مشاكل في التردد اللاسلكي)، فقد تسبب في حدوث تأخيرات في اتصال الشبكة. على سبيل المثال، إذا قمت بضبط المؤقت على القيمة القصوى 120 ثانية، فإن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ينتظر دقيقتين بين طلبات الهوية. إذا كان العميل يقوم بالتجوال ولم يتم تلقي الاستجابة من قبل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، فقد قمنا بإنشاء انقطاع لمدة دقيقتين على الأقل لهذا العميل. التوصيات الخاصة بهذا المؤقت هي 5. في هذا الوقت، لا يوجد سبب لوضع هذا المؤقت بأقصى قيمة له.
- **الحد الأقصى لعمليات إعادة محاولة EAP-Identity-Request:** يقصد ب Max Retries Value عدد المرات التي تقوم فيها وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بإرسال طلب الهوية إلى العميل، قبل إزالة إدخالها من MSCB. وبمجرد الوصول إلى الحد الأقصى لعمليات إعادة المحاولة، يرسل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) إطار إلغاء مصادقة إلى العميل، مما يفرض عليه إعادة تشغيل عملية EAP. القيمة المتاحة هي من 1 إلى 20. وبعد ذلك، سننظر في هذه المسألة بمزيد من التفصيل. الحد الأقصى لإعادة المحاولة يعمل مع مهلة الهوية. إذا تم تعيين مهلة هويتك إلى 120، ويحاول الحد الأقصى لإعادة المحاولة إلى 20 كم يستغرق 2400 (أو 120 \* 20). وهذا يعني أن إزالة العميل سوف تستغرق 40 دقيقة، ثم إعادة تشغيل عملية EAP. إذا

قمت بتعيين مهلة الهوية إلى 5، بقيمة الحد الأقصى لإعادة المحاولة 12، فسوف تستغرق 60 (أو 5 \* 12). خلافا للمثال السابق، تبقى دقيقة واحدة حتى تتم إزالة العميل ويتوجب عليه بدء EAP من جديد. التوصيات الخاصة بالحد الأقصى لعمليات إعادة المحاولة هي 12.

• **مهلة مفتاح EAPOL:** بالنسبة لقيمة مهلة EAPOL-Key، تكون القيمة الافتراضية ثانية واحدة أو 1000 مللي ثانية. وهذا يعني أنه عندما يتم تبادل مفاتيح EAPOL بين نقطة الوصول والعميل، فإن نقطة الوصول سترسل المفتاح وتنتظر حتى ثانية واحدة بشكل افتراضي حتى يتمكن العميل من الاستجابة. بعد انتظار قيمة الوقت المحددة، تعيد نقطة الوصول إرسال المفتاح مرة أخرى. يمكنك استخدام الأمر `config advanced eap eapol-key-timeout` لتغيير هذا الإعداد. تتراوح القيم المتوفرة في 6.0 بين 200 و 5000 مللي ثانية، بينما تسمح الرموز السابقة ل 6.0 بالقيم بين 1 و 5 ثوان. تذكر دائما أنه إذا كان لديك عميل لا يستجيب لمحاولة رئيسية، فإن تمديد الوقت للخارج يمكن أن يمنحهم وقتا أكثر قليلا للرد. ومع ذلك، قد يؤدي هذا أيضا إلى إطالة الوقت الذي يستغرقه عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)/نقطة الوصول لإلغاء مصادقة العميل حتى تبدأ عملية 802.1x بالكامل من جديد.

• **عمليات إعادة محاولة مفتاح Eapol:** بالنسبة لقيمة عمليات إعادة المحاولة الفصوى الخاصة ب EAPOL-Key، يكون الافتراضي هو 2. وهذا يعني أننا سنعيد محاولة المفتاح الأصلي للعميل مرتين. يمكن تغيير هذا الإعداد باستخدام الأمر `config advanced eap eapol-key retries`. تتراوح القيم المتاحة بين 0 و 4 محاولات. باستخدام القيمة الافتراضية لمهلة EAPOL-Key (أي ثانية واحدة) والقيمة الافتراضية لإعادة محاولة (EAPOL-Key) 2، سيتم تنفيذ العملية كما يلي إذا لم يستجب العميل لمحاولة المفتاح الأولية: ترسل نقطة الوصول محاولة مفتاح إلى العميل. تنتظر ثانية واحدة للرد. في حالة عدم وجود رد، يتم إرسال أول إعادة محاولة ل EAPOL-Key. تنتظر ثانية واحدة للرد. في حالة عدم وجود رد، يتم إرسال إعادة محاولة EAPOL-Key الثانية. في حالة عدم استجابة العميل حتى الآن واستيفاء قيمة إعادة المحاولة، يتم إلغاء مصادقة العميل. مرة أخرى، كما هو الحال مع مهلة EAPOL-Key، قد يكون توسيع قيمة إعادة محاولة EAPOL-Key مفيدا في بعض الظروف. ومع ذلك، قد يكون تعيينها إلى الحد الأقصى ضارا مرة أخرى لأن الرسالة التي يتم إلغاء المصادقة عليها قد تطول.

## [إستخراج ملف الحزمة من خادم ACS RADIUS لاستكشاف الأخطاء وإصلاحها](#)

إذا كنت تستخدم ACS كخادم RADIUS خارجي، يمكن استخدام هذا القسم لاستكشاف أخطاء التكوين وإصلاحها. الحزمة cab هو ملف zip يحتوي على كل الملفات الضرورية الضرورية in order to تحريت ACS بكفاءة. يمكنك استخدام أداة CSSupport.exe المساعدة لإنشاء الحزمة cab، أو يمكنك تجميع الملفات يدويا.

راجع قسم [إنشاء ملف packages.cab](#) في الحصول على معلومات الإصدار و AAA تصحيح الأخطاء ل Cisco Windows J Secure ACS للحصول على مزيد من المعلومات حول كيفية إنشاء ملف الحزمة واستخراجه من WCS.

## [معلومات ذات صلة](#)

- [مثال تكوين نقاط الوصول في الوضع Lightweight](#)
- [ترقية برنامج \(Wireless LAN Controller\) \(WLC\)](#)
- [مرجع أوامر وحدة تحكم شبكة LAN اللاسلكية من Cisco](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءن إلل دن تسمل