

RADIUS مداخل مداخل حساب ةي ج راخ بي و ة ق د اص م

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [مصادقة الويب الخارجية](#)
- [تكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\)](#)
- [تكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) ل Cisco Secure ACS](#)
- [تكوين شبكة WLAN على WLC لمصادقة الويب](#)
- [تكوين معلومات خادم الويب على WLC](#)
- [تكوين مصدر المحتوى الإضافي الآمن من Cisco](#)
- [تكوين معلومات المستخدم على ACS الآمن من Cisco](#)
- [تكوين معلومات WLC على ACS الآمن من Cisco](#)
- [عملية مصادقة العميل](#)
- [تكوين العميل](#)
- [عملية تسجيل دخول العميل](#)
- [التحقق من الصحة](#)
- [التحقق من مصدر المحتوى الإضافي](#)
- [التحقق من WLC](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [أوامر استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يشرح هذا المستند كيفية إجراء مصادقة ويب خارجية باستخدام خادم RADIUS خارجي.

المتطلبات الأساسية

المتطلبات

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

- معرفة أساسية بتكوين نقاط الوصول في الوضع (Lightweight) (LAPs) و Cisco WLCs
- معرفة كيفية إعداد خادم ويب خارجي وتكوينه
- معرفة كيفية تكوين ACS الآمن من Cisco

المكونات المستخدمة

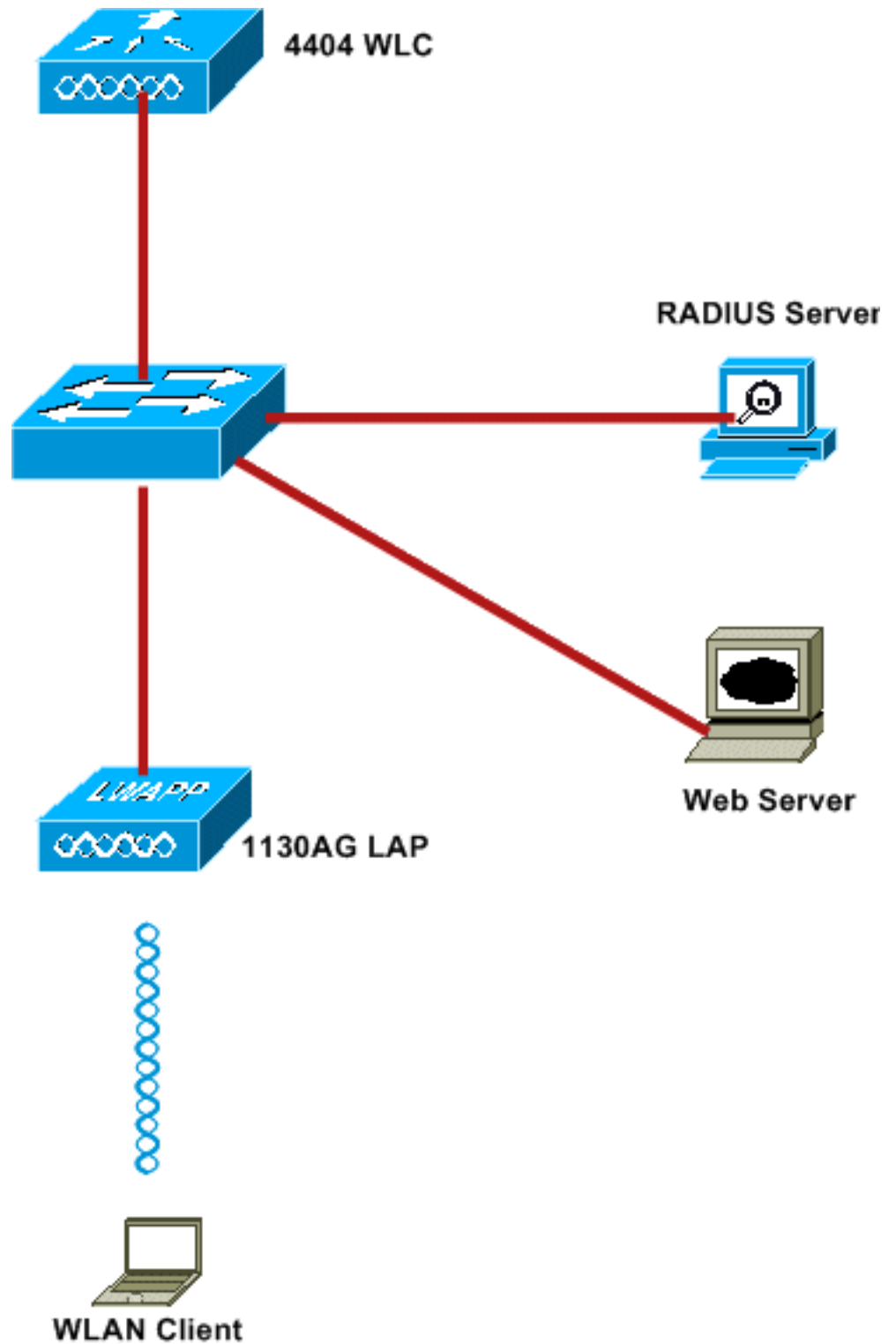
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة التحكم في شبكة LAN اللاسلكية التي تشغل الإصدار 5.0.148.0 من البرنامج الثابت
- نقطة الوصول في الوضع Lightweight من السلسلة Cisco 1232 Series LAP
- مهائئ العميل اللاسلكي 3.6.0.61 802.11a/b/g من Cisco
- خادم ويب خارجي الذي يستضيف صفحة تسجيل الدخول لمصادقة الويب
- Cisco Secure ACS الإصدار 4.1.1.24 من البرنامج الثابت

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.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



هذه هي عناوين IP المستخدمة في هذا المستند:

- يستخدم WLC عنوان IP 10.77.244.206
- LAP مسجل إلى WLC مع عنوان IP 10.77.244.199
- يستخدم خادم الويب عنوان IP 10.77.244.210
- يستخدم خادم Cisco ACS عنوان IP 10.77.244.196
- يستلم العميل عنوان IP من واجهة الإدارة التي تم تعيينها على الشبكة المحلية اللاسلكية (- WLAN) 10.77.244.208

[الاصطلاحات](#)

مصادقة الويب الخارجية

مصادقة الويب هي آلية مصادقة من الطبقة 3 تستخدم لمصادقة المستخدمين الضيوف للوصول إلى الإنترنت. لن يتمكن المستخدمون الذين تمت مصادقتهم باستخدام هذه العملية من الوصول إلى الإنترنت حتى يستكملوا عملية المصادقة بنجاح. للحصول على معلومات كاملة حول عملية مصادقة الويب الخارجية، اقرأ القسم عملية مصادقة الويب الخارجية الخاصة بالمستند مصادقة الويب الخارجية مع مثال تكوين وحدات تحكم الشبكة المحلية اللاسلكية.

في هذا المستند، ننظر إلى مثال تكوين، يتم فيه إجراء مصادقة الويب الخارجية باستخدام خادم RADIUS خارجي.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

في هذا المستند، نفترض أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه بالفعل ولديه نقطة وصول (LAP) مسجلة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يفترض هذا المستند كذلك أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم تكوينه للتشغيل الأساسي وأن نقاط الوصول في الوضع Lightweight تم تسجيلها إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). إذا كنت مستخدماً جديداً يحاول إعداد عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية باستخدام نقاط الوصول في الوضع Lightweight (LAP)، فارجع إلى تسجيل نقطة الوصول في الوضع Lightweight (LAP) إلى وحدة تحكم شبكة محلية لاسلكية (WLC). لعرض نقاط الوصول في الوضع Lightweight (LAPs) المسجلة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى لاسلكي > جميع نقاط الوصول (APs).

بمجرد تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للتشغيل الأساسي وتزويده بنقطة وصول واحدة أو أكثر مسجلة إليه، يمكنك تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لمصادقة الويب الخارجية باستخدام خادم ويب خارجي. في مثالنا، نستخدم إصدار Cisco ACS الآمن 4.1.1.24 كخادم RADIUS. أولاً، سنقوم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لخادم RADIUS هذا، ومن ثم سنبحث عن التكوين المطلوب على مصدر المحتوى الإضافي الآمن من Cisco لهذا الإعداد.

تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لـ Cisco Secure ACS

أنجزت هذا steps in order to أضفت ال RADIUS نادل على ال WLC:

1. من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC)، انقر فوق قائمة الأمان.
2. تحت قائمة AAA، انتقل إلى القائمة الفرعية RADIUS > المصادقة.
3. انقر فوق جديد، وأدخل عنوان IP الخاص بخادم RADIUS. في هذا المثال، عنوان IP الخاص بالخادم هو 10.77.244.196.
4. دخلت ال يشارك سر في ال WLC. يجب تكوين "السر المشترك" نفسه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
5. أختار إما ASCII أو hex لتنسيق سري مشترك. يجب إختيار نفس التنسيق على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
6. 1812 هو رقم المنفذ المستخدم لمصادقة RADIUS.
7. تأكد من تعيين خيار حالة الخادم إلى ممكن.
8. حدد مربع تمكين مستخدم الشبكة لمصادقة مستخدمي الشبكة.
9. طقطقة يطبق.

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The left sidebar is under 'Security' and expanded to 'RADIUS'. The main area is titled 'RADIUS Authentication Servers > New' and contains the following fields:

- Server Index (Priority): 2
- Server IP Address: 10.77.244.196
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled
- Support for RFC 3576: Enabled
- Server Timeout: 2 seconds
- Network User: Enable
- Management: Enable
- IPSec: Enable

تكوين شبكة WLAN على WLC لمصادقة الويب

تتمثل الخطوة التالية في تكوين شبكة WLAN لمصادقة الويب على WLC. أنجزت هذا steps in order to شكلت ال WLAN على WLC:

1. انقر فوق قائمة شبكات WLAN من واجهة المستخدم الرسومية (GUI) لوحدة التحكم، واختر جديد.
2. أختَر WLAN للنوع.
3. أدخل اسم توصيف ومعرف WLAN SSID من إختيارك، وانقر تطبيق. ملاحظة: WLAN SSID حساس لحالة الأحرف.

The screenshot shows the Cisco WLC configuration interface for creating a new WLAN. The left sidebar is under 'WLANs' and expanded to 'Advanced'. The main area is titled 'WLANs > New' and contains the following fields:

- Type: WLAN
- Profile Name: WLAN1
- WLAN SSID: WLAN1

4. تحت علامة التبويب عام، تأكد من أن خيار تمكين محدد لكل من الحالة و Broadcast SSID. تكوين شبكة

The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows WLANs > Edit. The main content area is titled 'WLANs > Edit' and has tabs for General, Security, QoS, and Advanced. The Security tab is active, showing the following configuration:

- Profile Name: WLAN1
- Type: WLAN
- SSID: WLAN1
- Status: Enabled
- Security Policies: [WPA2][Auth(002.1X)]
(Modifications done under security tab will appear after applying the changes.)
- Radio Policy: All
- Interface: management
- Broadcast SSID: Enabled

Foot Notes:

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

5. أخترت قارئ ل ال WLAN. بشكل خاص، يتم تعيين واجهة تم تكوينها في شبكة VLAN فريدة على الشبكة المحلية اللاسلكية (WLAN) حتى يستلم العميل عنوان IP في شبكة VLAN هذه. في هذا المثال، نستخدم الإدارة للواجهة.
6. أختار علامة التوجيه أمان.
7. تحت قائمة الطبقة 2، أختار لا شيء لأمان الطبقة 2.
8. تحت قائمة الطبقة 3، أختار لا شيء لأمان الطبقة 3. حدد خانة الاختيار نهج الويب، واختر المصادقة.

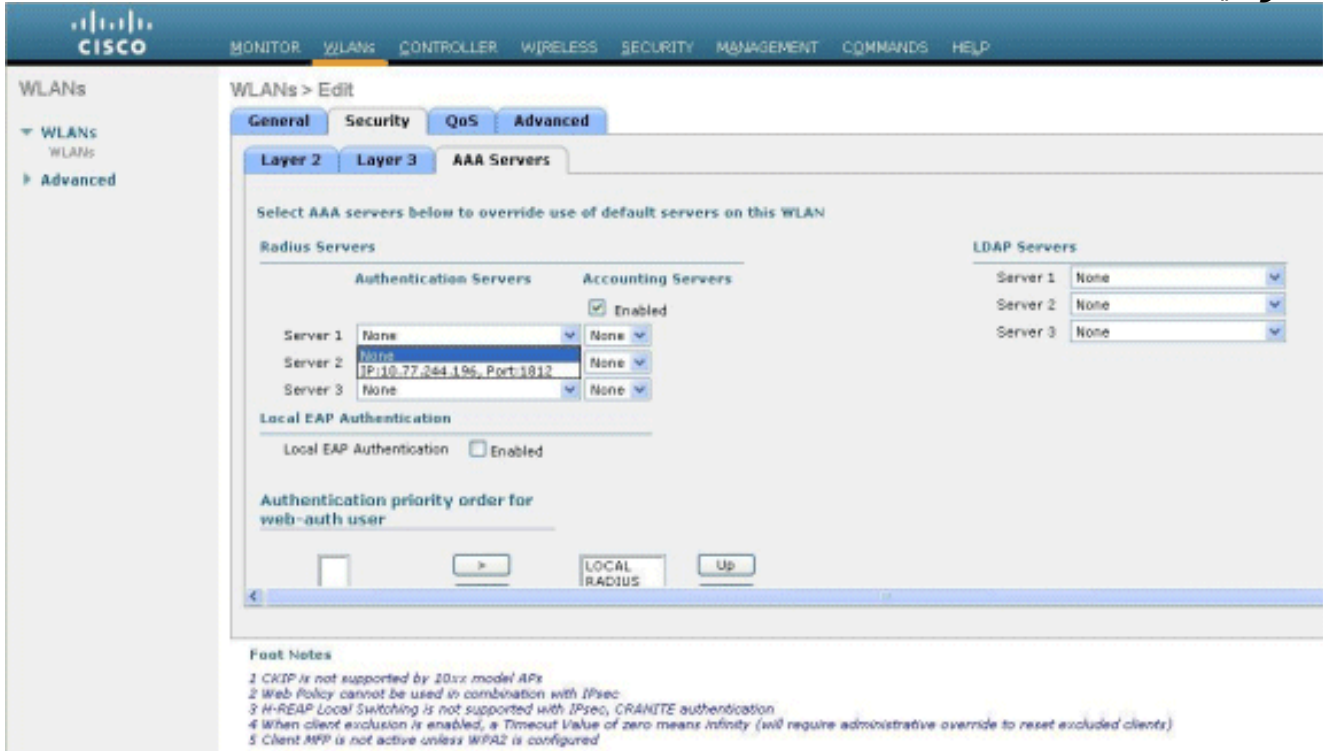
The screenshot shows the Cisco WLAN configuration interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows WLANs > Edit. The main content area is titled 'WLANs > Edit' and has tabs for General, Security, QoS, and Advanced. The Security tab is active, and the AAA Servers sub-tab is selected. The configuration is as follows:

- Layer 3 Security: None
- Web Policy 2
- Authentication
- Passthrough
- Conditional Web Redirect
- Splash Page Web Redirect
- Preauthentication ACL: None
- Over-ride Global Config: Enable

Foot Notes:

- 1 CKIP is not supported by 10xx model APs
- 2 Web Policy cannot be used in combination with IPsec
- 3 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
- 4 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
- 5 Client MFP is not active unless WPA2 is configured

9. تحت قائمة خوادم AAA، ل خادم المصادقة، اختر خادم RADIUS الذي تم تكوينه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) هذا. يجب أن تظل القوائم الأخرى بالقيم الافتراضية.



تكوين معلومات خادم الويب على WLC

يجب تكوين خادم ويب الذي يستضيف صفحة مصادقة الويب على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
قم بإجراء هذه الخطوات لتكوين خادم الويب:

1. انقر فوق علامة التبويب أمان. انتقل إلى مصادقة الويب < صفحة تسجيل الدخول إلى الويب.
2. تعيين نوع مصادقة الويب على أنه خارجي.
3. في حقل عنوان IP لخادم الويب، أدخل عنوان IP الخاص بالخادم الذي يستضيف صفحة مصادقة الويب، وانقر فوق إضافة خادم ويب. في هذا المثال، عنوان IP هو 10.77.244.196، والذي يظهر تحت خوادم الويب الخارجية.
4. أدخل عنوان URL لصفحة مصادقة الويب (في هذا المثال، http://10.77.244.196/login.html) في حقل عنوان URL.

The screenshot shows the Cisco Security configuration interface for the Web Login Page. The left sidebar contains a navigation menu with categories like AAA, Local EAP, Priority Order, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. The 'Web Auth' section is expanded, and 'Web Login Page' is selected. The main content area shows the following configuration:

- Web Authentication Type:** External (Redirect to external server)
- URL:** http://10.77.244.196/login.html
- External Web Servers:** A table with one entry: 10.77.244.196, with a 'Remove' button next to it.
- Web Server IP Address:** An empty text input field.
- Add Web Server:** A button to add a new web server.

تكوين مصدر المحتوى الإضافي الآمن من Cisco

في هذا المستند نفترض أن خادم ACS الآمن من Cisco مثبت بالفعل وأنه قيد التشغيل على جهاز. للحصول على مزيد من المعلومات حول كيفية إعداد Cisco Secure ACS، ارجع إلى [دليل التكوين لـ Cisco Secure ACS 4.2](#).

تكوين معلومات المستخدم على ACS الآمن من Cisco

أنجزت هذا steps in order to شكلت مستعمل على ال cisco يأمن ACS:

1. أخترت مستعمل setup من ال cisco يأمن ACS، دخلت username، وطققة يضيف/يحرر. في هذا المثال، المستخدم هو `user1`.



User Setup

Select

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

User:

List users beginning with letter/number:

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

[Back to Help](#)

2. بشكل افتراضي، يتم استخدام PAP لمصادقة العملاء. يتم إدخال كلمة المرور الخاصة بالمستخدم ضمن إعداد المستخدم < مصادقة كلمة المرور > Cisco PAP الآمن. تأكد من إختيار قاعدة بيانات ACS الداخلية لمصادقة كلمة المرور.

CISCO SYSTEMS User Setup

Edit

User: user1 (New User)

Account Disabled

Supplementary User Info ?

Real Name:

Description:

User Setup ?

Password Authentication:

(Dropdown)

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

Password:

Confirm Password:

Separate (CHAP/MS-CHAP/ARAP)

Password:

Confirm Password:

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

Group to which the user is assigned:

(Dropdown)

3. يجب تعيين مجموعة إلى المستخدم ينتمي إليها المستخدم. أختار المجموعة الافتراضية.
4. انقر على إرسال.

تكوين معلومات WLC على ACS الآمن من Cisco

أنجزت هذا steps in order to شكلت WLC معلومة على cisco يأمن ACS:

1. في واجهة المستخدم الرسومية (ACS)، انقر فوق علامة التبويب تكوين الشبكة، وانقر فوق إضافة إدخال.
2. تظهر الشاشة إضافة عميل AAA.
3. أدخل اسم العميل. في هذا المثال، نستخدم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
4. أدخل عنوان IP الخاص بالعميل. عنوان IP الخاص بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) هو 10.77.244.206.
5. أدخل مفتاح "سر مشترك" وتنسيق المفتاح. يجب أن يتطابق هذا مع الإدخال الذي تم إجراؤه في قائمة أمان WLC.
6. أخترت ASCII ل المفتاح مدخل تنسيق، أي ينبغي كنت ال نفس على ال WLC.
7. أخترت RADIUS (cisco Airespace) ل يصادق يستعمل in order to ثبتت البروتوكول يستعمل بين ال WLC و RADIUS نادل.
8. انقر فوق إرسال +

CISCO SYSTEMS Network Configuration

Add AAA Client

AAA Client Hostname: WLC

AAA Client IP Address: 10.77.244.206

Shared Secret: abc123

RADIUS Key Wrap

Key Encryption Key: []

Message Authenticator Code Key: []

Key Input Format: ASCII Hexadecimal

Authenticate Using: RADIUS (Cisco Airespace)

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

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

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

Submit Submit + Apply Cancel

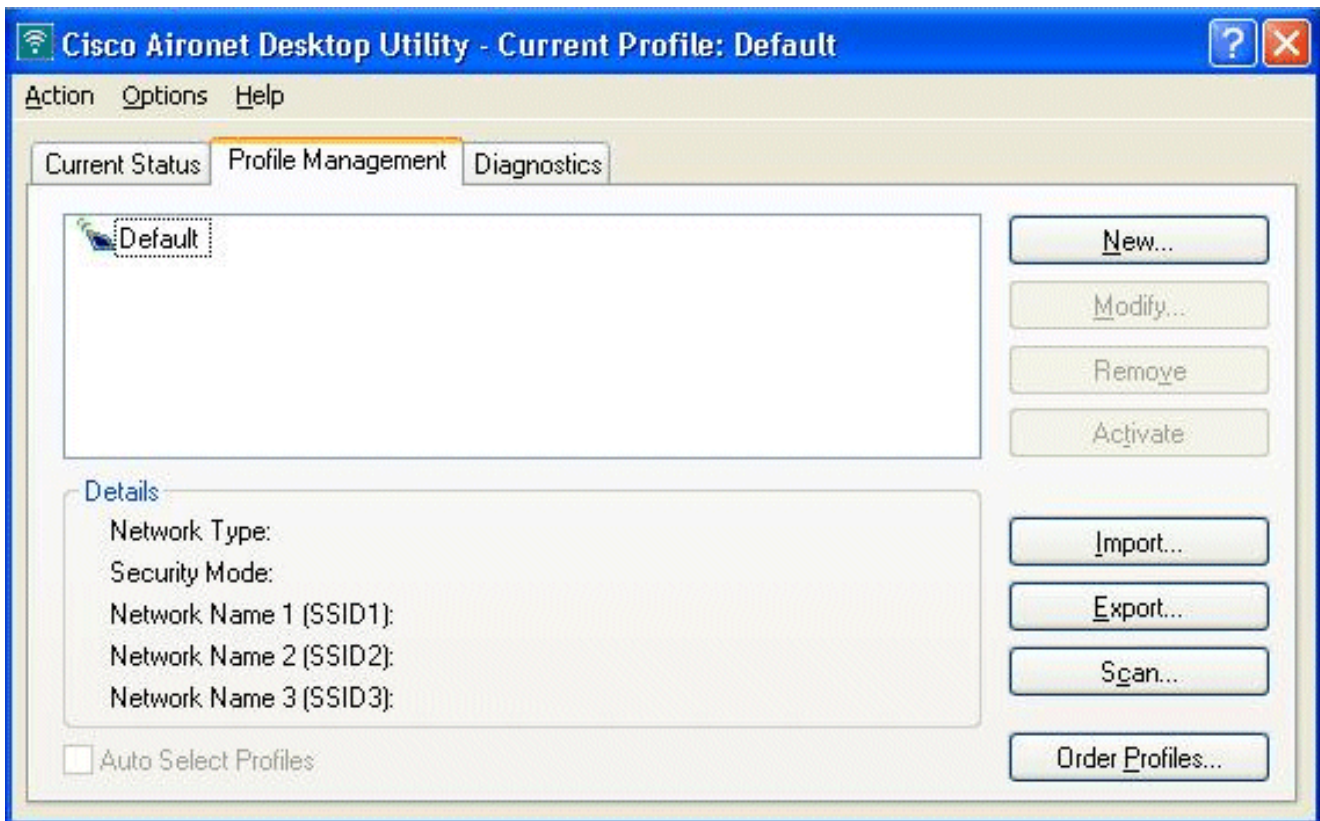
Back to Help

عملية مصادقة العميل

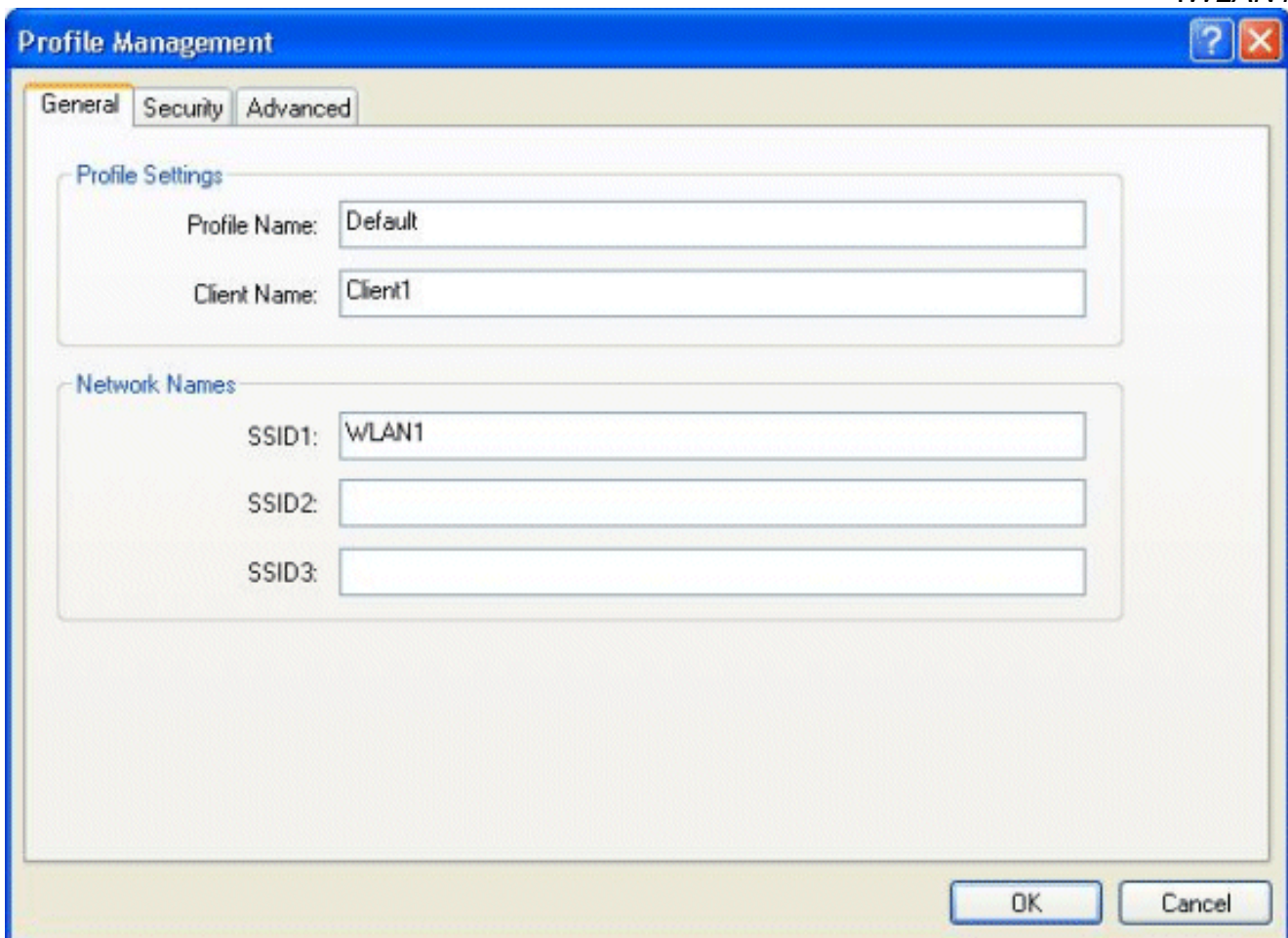
تكوين العميل

في هذا المثال، نستخدم الأداة المساعدة لسطح المكتب Cisco Aironet Desktop Utility لإجراء مصادقة الويب. قم بإجراء هذه الخطوات لتكوين الأداة المساعدة لسطح المكتب Aironet.

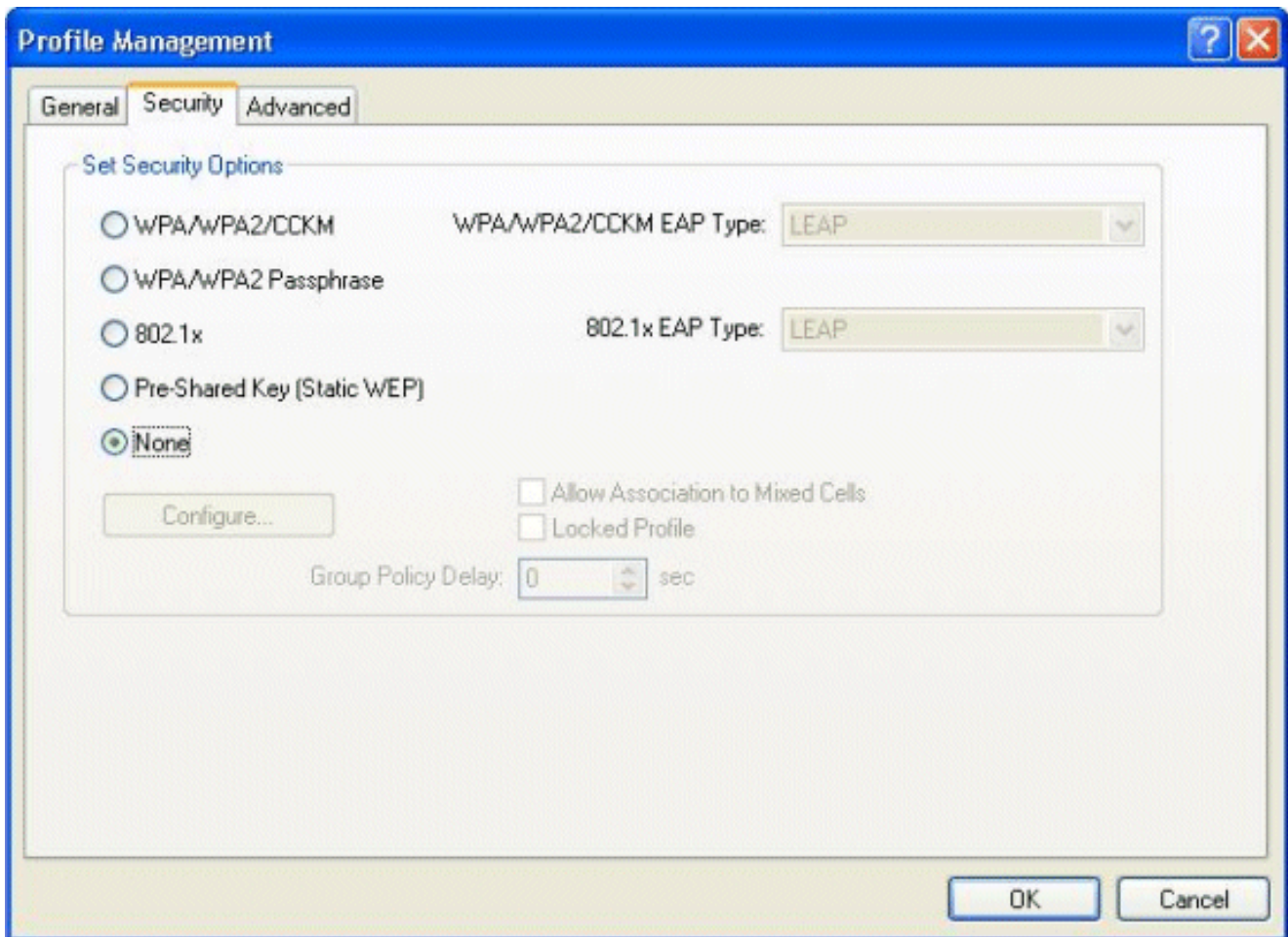
1. افتح أداة Aironet Desktop Utility من البداية < Cisco Aironet < أداة Aironet Desktop Utility.
2. انقر على علامة تبويب إدارة التوصيفات.



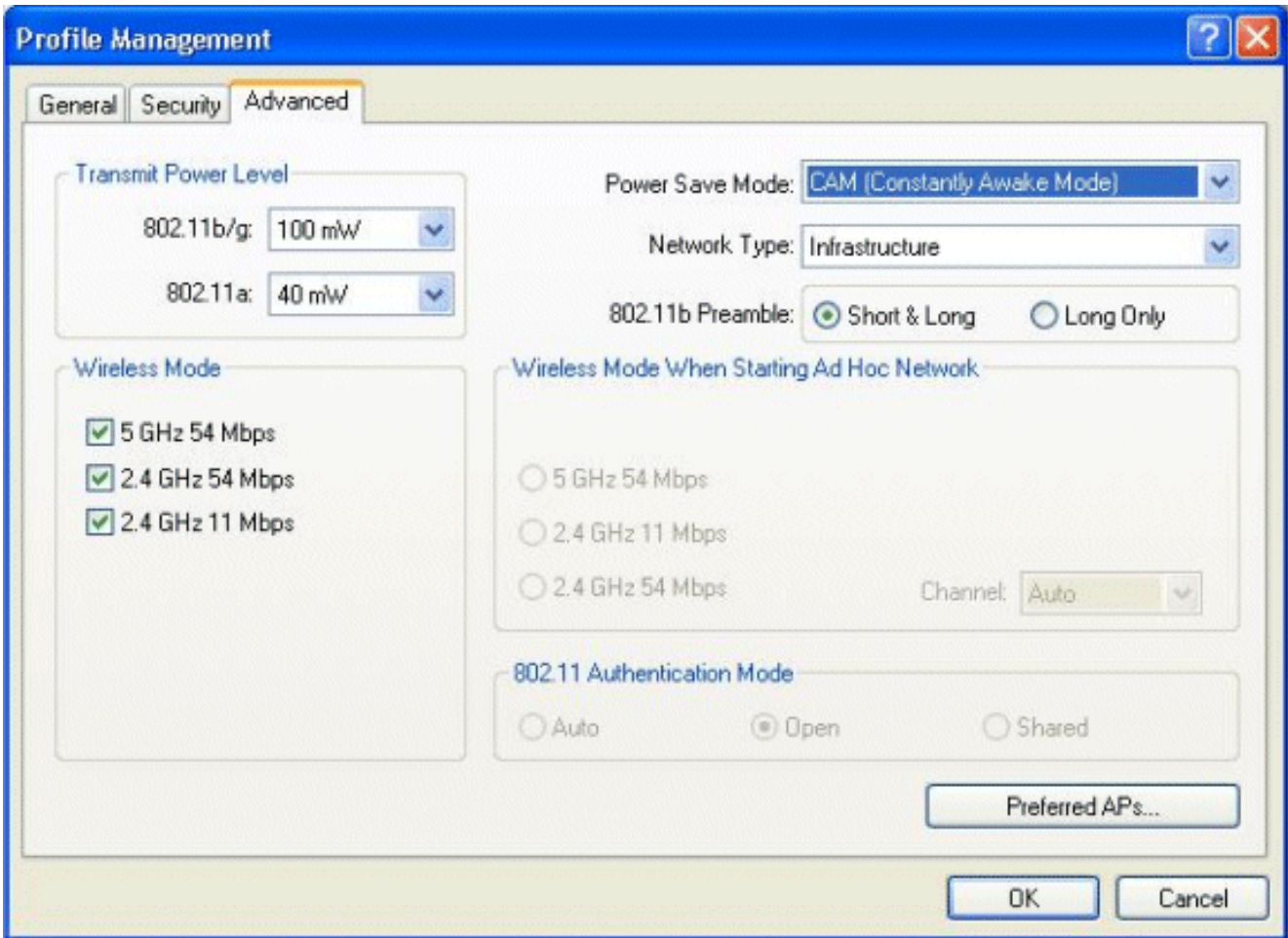
3. أختار ملف التخصيص الافتراضي، وانقر تعديل. انقر فوق علامة التبويب عام. تشكيل اسم توصيف. في هذا المثال، يتم استخدام الافتراضي. قم بتكوين SSID تحت أسماء الشبكة. في هذا المثال، يتم استخدام WLAN1.



ملاحظة: SSID حساس لحالة الأحرف ويجب أن يطابق شبكة WLAN التي تم تكوينها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). انقر فوق علامة التبويب أمان. أختار بلا كأمان لمصادقة الويب.



انقر فوق علامة التبويب **خيارات متقدمة**. تحت قائمة **الوضع اللاسلكي**، اختر التردد الذي يتصل عنده العميل اللاسلكي بنقطة الوصول في الوضع اللاسلكي (LAP). اخترت تحت ال **transmit طاقة مستوى**، الطاقة أن يكون شكلت على ال WLC. أترك القيمة الافتراضية لوضع حفظ الطاقة. اختر **بنية أساسية** كنوع الشبكة. تعيين دياجة 802.11b على أنها **قصيرة وطويلة** لتحقيق توافق أفضل. وانقر فوق **.OK**

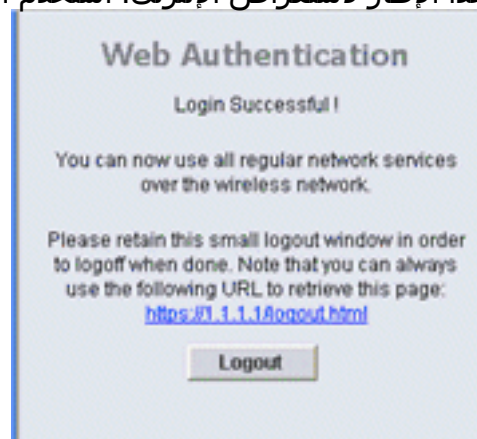


4. بمجرد تكوين ملف التعريف على برنامج العميل، يتم اقتران العميل بنجاح ويستلم عنوان IP من تجمع VLAN الذي تم تكوينه لمواجهة الإدارة.

عملية تسجيل دخول العميل

يشرح هذا القسم كيفية حدوث تسجيل دخول العميل.

1. افتح نافذة المستعرض وأدخل أي عنوان URL أو عنوان IP. يؤدي هذا إلى جلب صفحة مصادقة الويب إلى العميل. إذا كانت وحدة التحكم تقوم بتشغيل أي إصدار أقدم من 3.0، فيجب على المستخدم إدخال <https://1.1.1.1/login.html> لإظهار صفحة مصادقة الويب. تظهر نافذة تنبيه أمان.
2. طغطة نعم in order to باشرت.
3. عندما تظهر نافذة تسجيل الدخول، أدخل اسم المستخدم وكلمة المرور اللذين تم تكوينهما على خادم RADIUS. إذا نجح تسجيل دخولك، فسترى نافذتي مستعرض. الإطار الأكبر يشير إلى تسجيل دخول ناجح، ويمكنك هذا الإطار لاستعراض الإنترنت. أستخدم الإطار الأصغر لتسجيل الخروج عند اكتمال استخدامك لشبكة



الضيوف.

التحقق من الصحة

من أجل مصادقة ويب ناجحة، تحتاج إلى التحقق من تكوين الأجهزة بطريقة مناسبة. يشرح هذا القسم كيفية التحقق من الأجهزة المستخدمة في العملية.

التحقق من مصدر المحتوى الإضافي

1. انقر فوق إعدادات المستخدم، ثم انقر فوق سرد جميع المستخدمين في واجهة المستخدم الرسومية (ACS).

The screenshot shows the Cisco ACS User Setup interface. The left sidebar contains navigation options: 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, and Online Documentation. The main area is titled 'User Setup' and 'Select'. It features a search box for 'User:' with 'Find' and 'Add/Edit' buttons. Below is a list of users starting with a letter/number, with a 'List all users' button highlighted. At the bottom, there is a 'Remove Dynamic Users' button and a 'Back to Help' button.

تأكد من تمكين حالة المستخدم ومن تعيين المجموعة الافتراضية للمستخدم.

User List

User	Status	Group	Network Access Profile
user1	Enabled	Default Group (2 users)	(Default)

2. انقر فوق علامة التبويب تكوين الشبكة، وابحث في جدول عملاء AAA للتحقق من تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA.

CISCO SYSTEMS Network Configuration

Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
wlc1	10.77.244.206	RADIUS (Cisco Airespace)

Add Entry Search

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
TS-Web	10.77.244.196	CiscoSecure ACS

Add Entry Search

Proxy Distribution Table

Character String	AAA Servers	Strip	Account
(Default)	TS-Web	No	Local

Add Entry Sort Entries

[Back to Help](#)

التحقق من WLC

1. طقطقت ال WLANs قائمة من ال WLC GUI. تأكد من إدراج شبكة WLAN المستخدمة لمصادقة الويب في الصفحة. تأكد من تمكين حالة المسؤول لشبكة WLAN. تأكد من أن سياسة الأمان للشبكة المحلية اللاسلكية (WLAN) تعرض مصادقة الويب.

CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

WLANs

WLANs

Advanced

Profile Name	Type	WLAN SSID	Admin Status	Security Policies
WLAN1	WLAN	WLAN1	Enabled	Web-Auth

2. انقر فوق قائمة الأمان من واجهة المستخدم الرسومية (GUI) الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC). تأكد من إدراج مصدر المحتوى الإضافي الآمن من Cisco (10.77.244.196) في الصفحة. تأكد من تحديد مربع مستخدم الشبكة. تأكد من أن المنفذ هو 1812 وأن حالة المسؤول ممكنة.

Security

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

استكشاف الأخطاء وإصلاحها

هناك العديد من الأسباب التي تجعل مصادقة ويب غير ناجحة. يشرح المستند [استكشاف أخطاء مصادقة الويب وإصلاحها على وحدة تحكم شبكة محلية لاسلكية \(WLC\)](#) بشكل واضح هذه الأسباب بالتفصيل.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى [معلومات مهمة عن أوامر تصحيح الأخطاء](#) قبل أن تستخدم أوامر debug هذه.

Telnet في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) وأصدر هذه الأوامر لاستكشاف أخطاء المصادقة وإصلاحها:

debug aaa all enable •

```

Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Successful transmission of Authentic
ation Packet (id 1) to 10.77.244.196:1812, proxy state 00:40:96:ac:dd:05-00:01
Fri Sep 24 13:59:52 2010: 00000000: 01 01 00 73 00 00 00 00 00 00 00 00 00 00 0
.....s... 00 0
Fri Sep 24 13:59:52 2010: 00000010: 00 00 00 00 01 07 75 73 65 72 31 02 12 93 c
user1....f..... 66 3
Fri Sep 24 13:59:52 2010: 00000030: 75 73 65 72 31
user1
Fri Sep 24 13:59:52 2010: ****Enter processIncomingMessages: response code=2
Fri Sep 24 13:59:52 2010: ****Enter processRadiusResponse: response code=2
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Access-Accept received from RADIUS s
erver 10.77.244.196 for mobile 00:40:96:ac:dd:05 receiveId = 0
Fri Sep 24 13:59:52 2010: AuthorizationResponse: 0x12238db0
Fri Sep 24 13:59:52 2010: structureSize.....89
Fri Sep 24 13:59:52 2010: resultCode.....0
Fri Sep 24 13:59:52 2010: protocolUsed.....0x0
0000001
:Fri Sep 24 13:59:52 2010: proxyState.....00
AC:DD:05-00:00:40:96
:Fri Sep 24 13:59:52 2010: Packet contains 2 AVPs
.....Fri Sep 24 13:59:52 2010: AVP[01] Framed-IP-Address
(0xffffffff (-1) (4 bytes)....
.....Fri Sep 24 13:59:52 2010: AVP[02] Class
(CACS:0/5183/a4df4ce/user1 (25 bytes)....

```

```

Fri Sep 24 13:59:52 2010: Authentication failed for user1, Service Type: 0
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Applying new AAA override for station
                                n 00:40:96:ac:dd:05
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Override values for station 00:40:96
                                ac:dd:05:
                                source: 48, valid bits: 0x1
qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout: -1

                                dataAvgC: -1, rTAvgC: -1, dataBurstC: -1, rTimeBurstC: -1
, '':vlanIfName
                                :aclName
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Unable to apply override policy for
                                station 00:40:96:ac:dd:05 - VapAllowRadiusOverride is FALSE
Fri Sep 24 13:59:52 2010: 00:40:96:ac:dd:05 Sending Accounting request (0) for s
                                tation 00:40:96:ac:dd:05
                                Fri Sep 24 13:59:52 2010: AccountingMessage Accounting Start: 0x1500501c
                                :Fri Sep 24 13:59:52 2010: Packet contains 12 AVPs
.....Fri Sep 24 13:59:52 2010: AVP[01] User-Name
                                (user1 (5 bytes.....
.....Fri Sep 24 13:59:52 2010: AVP[02] Nas-Port
                                (0x00000002 (2) (4 bytes.....
.....Fri Sep 24 13:59:52 2010: AVP[03] Nas-IP-Address
                                (0x0a4df4ce (172881102) (4 bytes.....
.....Fri Sep 24 13:59:52 2010: AVP[04] Framed-IP-Address
                                (0x0a4df4c7 (172881095) (4 bytes.....

```

enable debug aaa detail •

يتم سرد محاولات المصادقة الفاشلة في القائمة الموجودة في التقارير والنشاط < محاولات فاشلة.

معلومات ذات صلة

- [مثال تكوين مصادقة الويب لوحدة تحكم الشبكة المحلية \(LAN\) اللاسلكية](#)
- [أستكشاف أخطاء مصادقة الويب وإصلاحها على وحدة تحكم شبكة محلية لاسلكية \(WLC\)](#)
- [مثال تكوين المصادقة الخارجية للويب مع وحدات تحكم الشبكة المحلية \(LAN\) اللاسلكية](#)
- [مصادقة الويب باستخدام LDAP على مثال تكوين وحدات تحكم الشبكة المحلية \(LAN\) اللاسلكية \(WLCs\)](#)
- [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