

# ادانتسا WLAN ةكبش ىلإ لوصولا دييقت ACS نيوكت لاثم و WLC مادختساب SSID ىلإ Cisco نم نم آلا

## المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[معلومات أساسية](#)

[Network Setup \(إعداد الشبكة\)](#)

[التكوين](#)

[تكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\)](#)

[تكوين مصدر المحتوى الإضافي الآمن من Cisco](#)

[تكوين العميل اللاسلكي والتحقق](#)

[استكشاف الأخطاء وإصلاحها](#)

[أوامر استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

## [المقدمة](#)

يقدم هذا المستند مثالا للتكوين لتقييد وصول كل مستخدم إلى شبكة WLAN استنادا إلى معرف مجموعة الخدمة (SSID).

## [المتطلبات الأساسية](#)

### [المتطلبات](#)

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

- معرفة كيفية تكوين وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) ونقطة الوصول في الوضع Lightweight (LAP) للتشغيل الأساسي
- معرفة أساسية حول كيفية تكوين خادم التحكم في الوصول الآمن (ACS) من Cisco
- معرفة بروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) وطرائق الأمان اللاسلكية

### [المكونات المستخدمة](#)

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

- Cisco 2000 Series WLC الذي يشغل البرنامج الثابت 4.0
- نقطة الوصول في الوضع Lightweight من السلسلة Cisco 1000 Series LAP
- خادم ACS الآمن من Cisco، الإصدار 3.2
- مهائى العميل اللاسلكي Cisco 802.11a/b/g الذي يشغل البرنامج الثابت 2.6
- الإصدار 2.6، (Cisco Aironet Desktop Utility (ADU)

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](#)

باستخدام الوصول إلى شبكة WLAN المستندة إلى SSID، يمكن مصادقة المستخدمين استناداً إلى SSID الذي يستخدمونه للاتصال بشبكة WLAN. يتم استخدام خادم ACS الآمن من Cisco لمصادقة المستخدمين. تحدث المصادقة في مرحلتين على مصدر المحتوى الإضافي الآمن من Cisco:

1. مصادقة EAP

2. تستند مصادقة SSID إلى قيود الوصول إلى الشبكة (NARs) على ACS الآمن من Cisco

في حالة نجاح المصادقة المستندة إلى EAP و SSID، يسمح للمستخدم بالوصول إلى الشبكة المحلية اللاسلكية (WLAN) ولا سيتم فصل المستخدم.

يستخدم مصدر المحتوى الإضافي الآمن من Cisco ميزة قوائم التحكم في الوصول (NARs) لتقييد وصول المستخدم استناداً إلى NAR. SSID هو تعريف، تضعه في ACS الآمن من Cisco، للشروط الإضافية التي يجب تليتها قبل أن يتمكن المستخدم من الوصول إلى الشبكة. يطبق Cisco Secure ACS هذه الشروط باستخدام معلومات من السمات المرسله من قبل عملاء AAA لديك. على الرغم من وجود طرق عديدة يمكنك من خلالها إعداد قوائم التحكم في الوصول (NARs)، إلا أنها جميعاً تستند إلى معلومات السمة المطابقة التي يرسلها عميل AAA. لذلك، يجب أن تفهم تنسيق ومحتوى السمات التي يرسلها عملاء AAA إذا كنت تريد استخدام قوائم التحكم في الوصول (NARs) الفعالة.

عندما تقوم بإنشاء وحدة مكافحة الحرائق، يمكنك إختيار إذا ما كان المرشح يعمل بشكل إيجابي أو سلبي. هذا يعني أنك في قائمة التحكم في الوصول للبنية الأساسية (NAR) تحدد ما إذا كنت تسمح بالوصول إلى الشبكة أو تمنعه بناء على مقارنة المعلومات المرسله من عملاء AAA بالمعلومات المخزنة في قائمة التحكم في الوصول للبنية الأساسية (NAR). ومع ذلك، إذا لم تواجه وحدة التحكم في الشبكة (NAR) معلومات كافية لتشغيلها، فإنها تقوم بالإعدادات الافتراضية لرفض الوصول.

يمكنك تحديد NAR لمستخدم معين أو مجموعة مستخدمين معينين وتطبيقه على. راجع [التقرير الرسمي لقيود الوصول إلى الشبكة](#) للحصول على مزيد من المعلومات.

يدعم مصدر المحتوى الإضافي الآمن من Cisco نوعين من عوامل تصفية NAR:

1. **عوامل التصفية المستندة إلى IP** — تعمل عوامل تصفية NAR المستندة إلى IP على الحد من الوصول استناداً إلى عناوين IP الخاصة بعميل المستخدم النهائي و عميل AAA. راجع [عوامل تصفية NAR المستندة إلى IP](#) للحصول على مزيد من المعلومات حول هذا النوع من عوامل تصفية NAR.
2. **عوامل تصفية غير قائمة على IP** — تعمل عوامل تصفية NAR غير المستندة إلى IP على الحد من الوصول استناداً إلى مقارنة سلسلة بسيطة لقيمة تم إرسالها من عميل AAA. يمكن أن تكون القيمة رقم معرف سطر الاتصال (CLI) أو رقم خدمة التعرف على الرقم المطلوب (DNIS) أو عنوان MAC أو أي قيمة أخرى تنشأ من العميل. لتشغيل هذا النوع من NAR، يجب أن تتطابق القيمة الواردة في وصف NAR تماماً مع القيمة المرسله

من العميل، بما في ذلك أي تنسيق يتم استخدامه. على سبيل المثال، (217) 4534-555 لا يطابق 217-555-4534. ارجع إلى [حول عوامل تصفية NAR غير المستندة إلى IP](#) للحصول على مزيد من المعلومات حول هذا النوع من عوامل تصفية NAR.

يستخدم هذا المستند عوامل التصفية غير المستندة إلى IP لإجراء مصادقة تستند إلى SSID. عامل تصفية NAR غير المستند إلى IP (أي عامل تصفية NAR القائم على DNIS/CLI) هو قائمة بمواقع الاتصال/نقاط الوصول المسموح بها أو المرفوضة التي يمكنك استخدامها في تقييد عميل AAA عندما لا يكون لديك اتصال يستند إلى IP. تستخدم ميزة NAR غير المستندة إلى IP بشكل عام رقم CLI ورقم DNIS. هناك إستثناءات في استخدام حقول DNIS/CLI. يمكنك إدخال اسم SSID في حقل DNIS والمصادقة المستندة إلى SSID. وذلك لأن عنصر التحكم في الشبكة المحلية اللاسلكية يرسل سمة DNIS، اسم SSID، إلى خادم RADIUS. لذلك إذا قمت بإنشاء NAR DNIS في المستخدم أو المجموعة، يمكنك إنشاء تقييدات SSID لكل مستخدم.

إذا كنت تستخدم RADIUS، فإن حقول NAR المدرجة هنا تستخدم القيم التالية:

- **عميل AAA** — عنوان NAS-IP (السمة 4) أو، في حالة عدم وجود عنوان NAS-IP، يتم استخدام معرف NAS (سمة 32 RADIUS).
  - **المنفذ** — يتم استخدام منفذ NAS-Port (السمة 5) أو، إذا لم يكن منفذ NAS موجودا، NAS-port-ID (attribute 87).
  - **CLI** — يتم استخدام معرف محطة الاتصال (السمة 31).
  - **DNIS** — يتم استخدام معرف المحطة المستدعي (السمة 30).
- ارجع إلى [تقييدات الوصول إلى الشبكة](#) للحصول على مزيد من المعلومات حول استخدام NAR.

ونظرا لأن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) يرسل سمة DNIS واسم SSID، يمكنك إنشاء تقييدات SSID لكل مستخدم. في حالة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، تحتوي حقول NAR على القيم التالية:

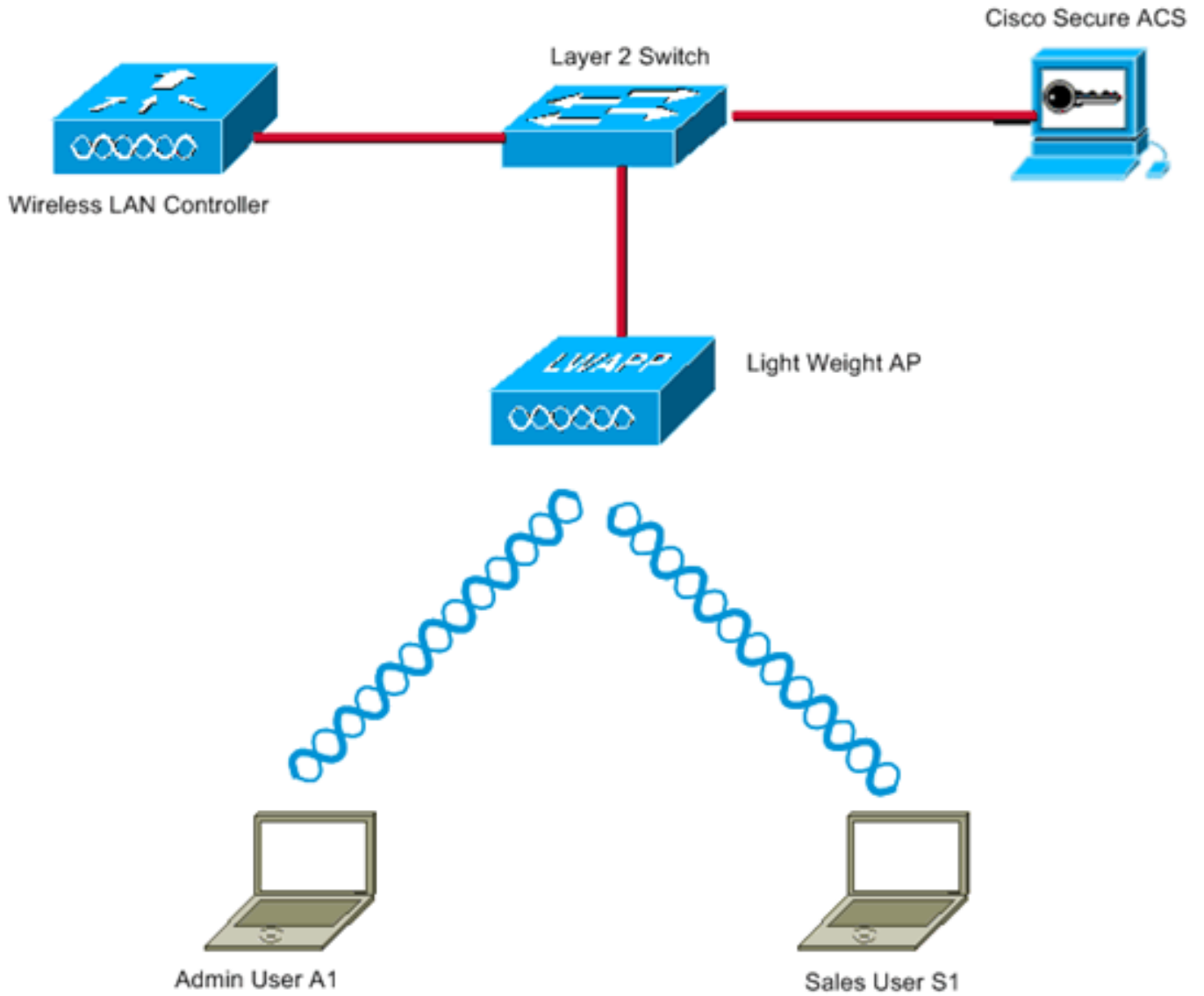
- **عميل AAA** — عنوان IP WLC
- **المنفذ** — \*
- **واجهة سطر الأوامر** — \*
- **DNIS** — \*ssidname

ويقدم باقي هذا المستند مثالا للتكوين حول كيفية تحقيق ذلك.

## [Network Setup \(إعداد الشبكة\)](#)

في هذا المثال، تم تسجيل WLC في نقطة الوصول (LAP Lightweight). يتم استخدام شبكتي WLAN. توجد شبكة محلية لاسلكية (WLAN) واحدة لمستخدمي قسم "الإدارة" بينما تكون شبكة WLAN الأخرى لمستخدمي قسم المبيعات. يتصل العميل اللاسلكي A1 (مستخدم المسؤول) و S1 (مستخدم المبيعات) بالشبكة اللاسلكية. أنت تحتاج أن يشكل ال WLC و RADIUS نادل بطريقة أن المسؤول مستعمل A1 يستطيع أن ينفذ فقط ال WLAN مدير و هو يقيد وصول إلى ال WLAN مبيعات و البائع S1 ينبغي كنت يمكن أن ينفذ ال WLAN مبيعات وينبغي يتلقى يقيد وصول إلى ال WLAN Admin. يستخدم جميع المستخدمين مصادقة LEAP كطريقة مصادقة من الطبقة 2.

**ملاحظة:** يفترض هذا المستند أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) مسجل لوحدة التحكم. إذا كنت جديدا في WLC ولا تعرف كيفية تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) للعملية الأساسية، فارجع إلى [تسجيل نقطة الوصول في الوضع \(LAP Lightweight\) إلى وحدة تحكم شبكة محلية لاسلكية \(WLC\)](#).



WLC Management Interface IP address : 172.16.1.30/16

WLC AP-Manager Interface IP address: 172.16.1.31/16

Cisco Secure ACS server IP address: 172.16.1.60/16

SSID for the Admin department users : Admin

SSID for Sales department users: Sales

## التكوين

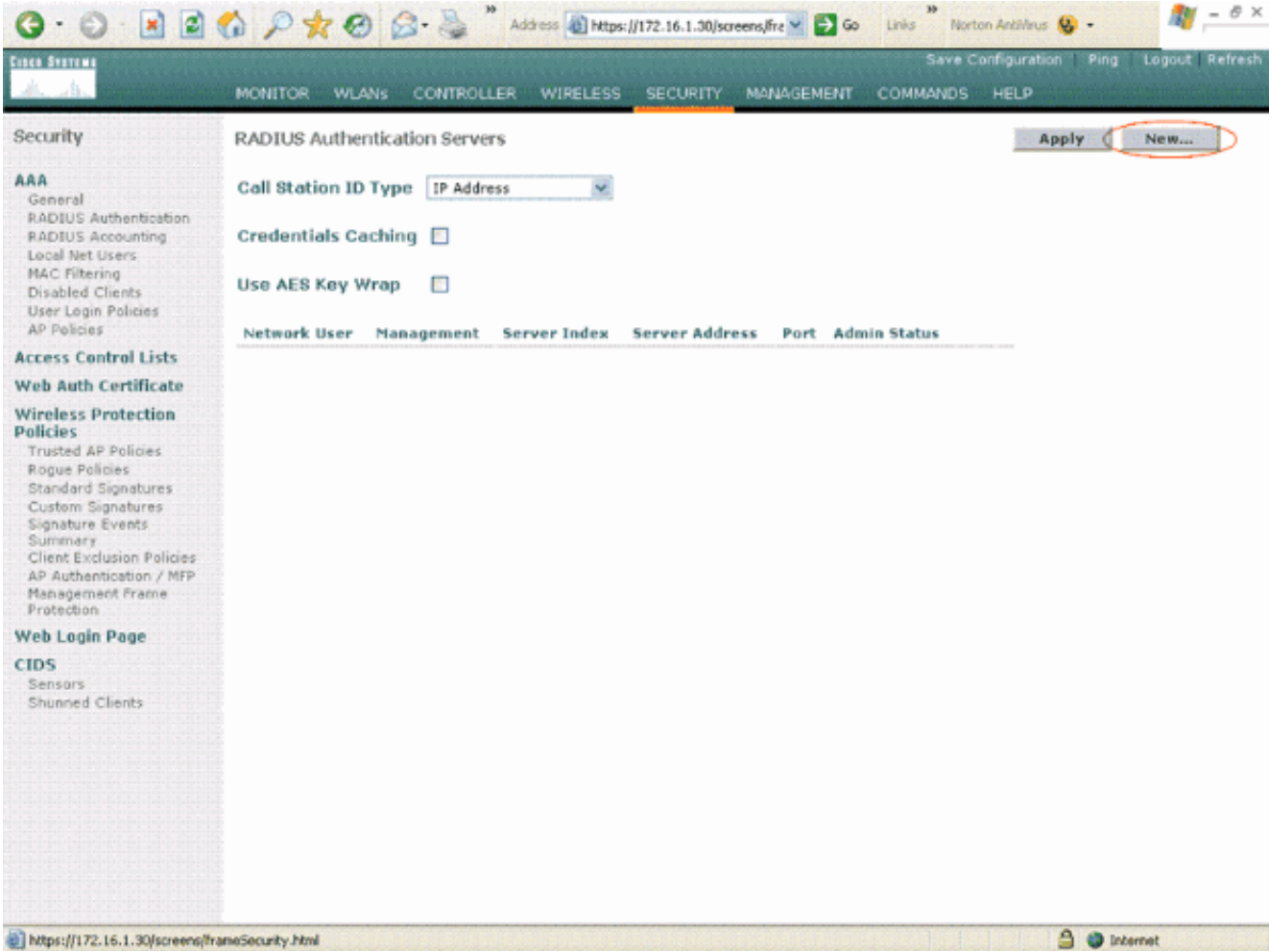
لتكوين الأجهزة لهذا الإعداد، يجب:

1. [قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\) لشبكتي WLAN وخادم RADIUS.](#)
2. [قم بتكوين مصدر المحتوى الإضافي الآمن من Cisco.](#)
3. [قم بتكوين العملاء اللاسلكيين والتحقق من الصحة.](#)

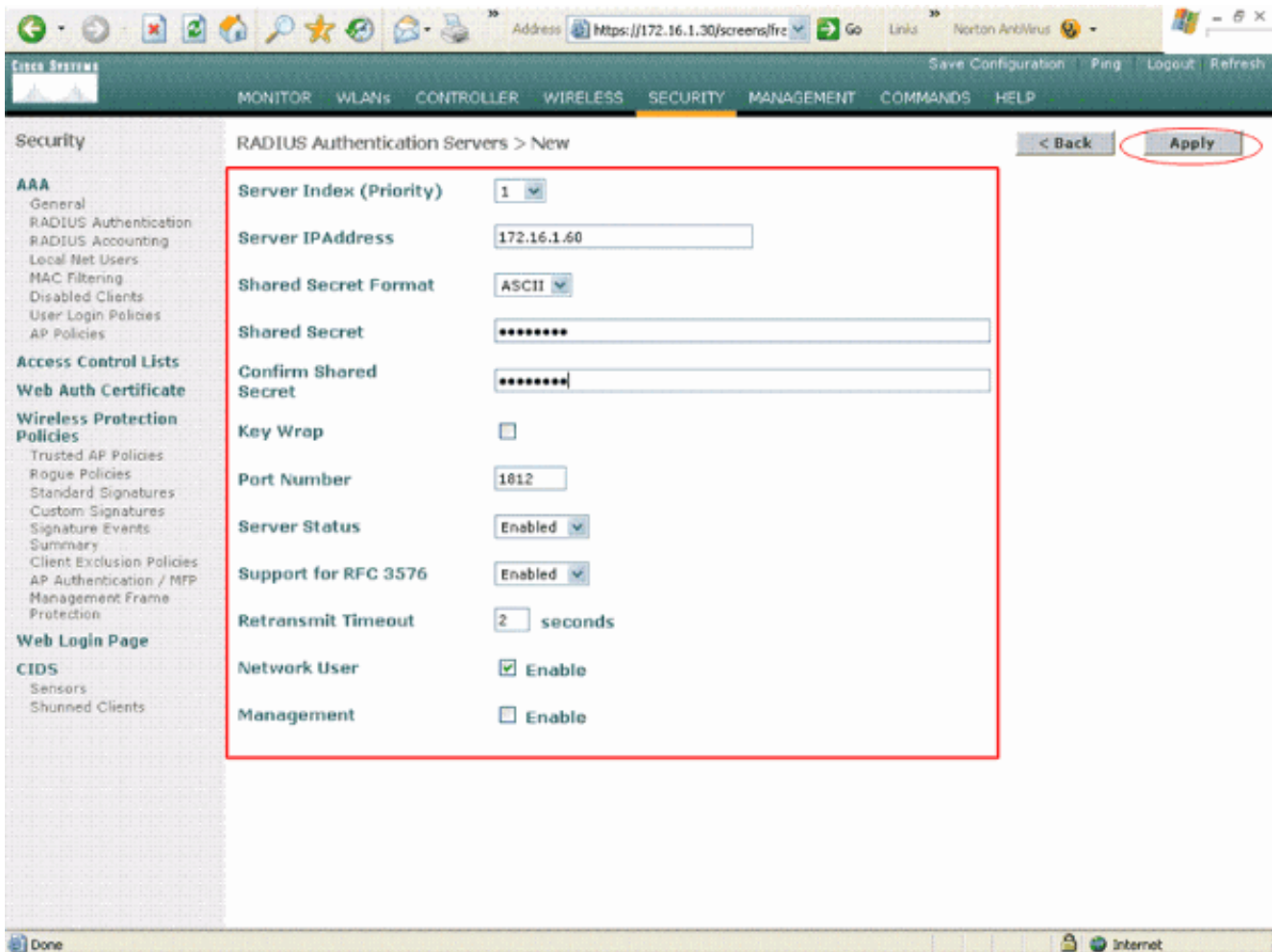
## [تكوين عنصر التحكم في الشبكة المحلية اللاسلكية \(WLC\)](#)

أتمت هذا steps in order to شكلت ال WLC ل هذا إعداد:

1. يلزم تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإعادة توجيه بيانات اعتماد المستخدم إلى خادم RADIUS خارجي. يتحقق خادم RADIUS الخارجي (Cisco Secure ACS) في هذه الحالة من مسوغات المستخدم ويوفر الوصول إلى العملاء اللاسلكيين. أكمل الخطوات التالية: اخترت أمن <RADIUS صحة هوية من الجهاز تحكم al عرضت ال RADIUS صحة هوية نادل صفحة.

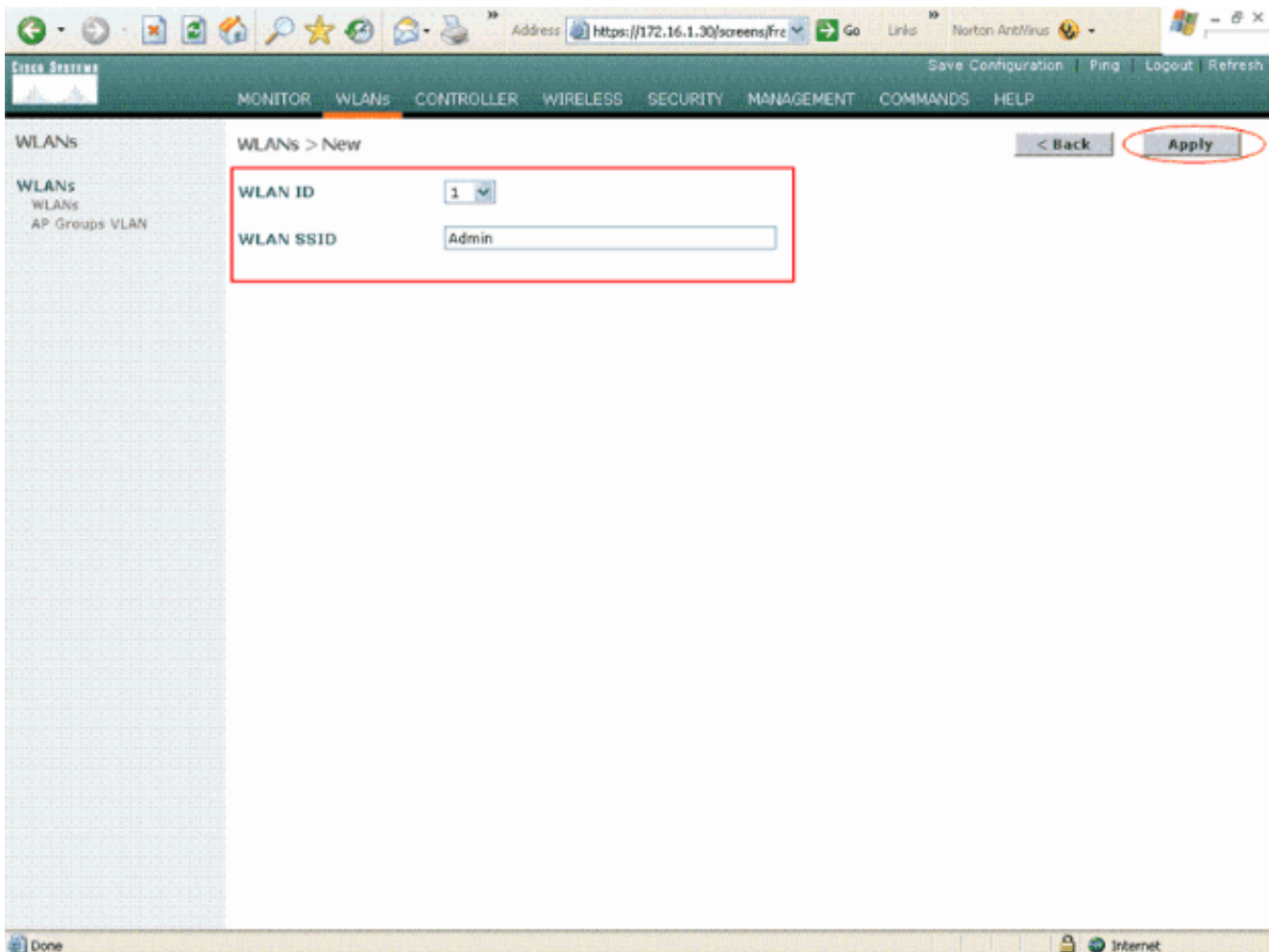


انقر فوق جديد لتحديد معلمات خادم RADIUS. وتتضمن هذه المعلمات عنوان IP لخادم RADIUS والسر المشترك ورقم المنفذ وحالة الخادم. تحدد خانة الاختيار الخاصة بمستخدم الشبكة وإدارتها ما إذا كانت المصادقة المستندة إلى RADIUS تنطبق على الإدارة ومستخدمي الشبكة. يستعمل هذا مثال ال cisco يأمن ACS كخادم RADIUS مع عنوان .172.16.1.60



طقطقة يطبق.

2. قم بتكوين شبكة WLAN واحدة لقسم "الإدارة" باستخدام مسؤول SSID وشبكة WLAN الأخرى لقسم المبيعات باستخدام مبيعات SSID. أتمت هذا steps in order to أنجزت هذا: طقطقت WLANs من الجهاز تحكم gui in order to خلقت WLAN. يظهر نافذة WLANs. تسرد هذه النافذة شبكات WLAN التي تم تكوينها على وحدة التحكم. طقطقت جديد in order to شكلت WLAN جديد. يقوم هذا المثال بإنشاء مسؤول مسمى WLAN لقسم "الإدارة" ومعرف WLAN هو 1. طقطقة يطبق.



في نافذة **WLAN** < تحرير، قم بتعريف المعلمات الخاصة بالشبكة المحلية اللاسلكية (WLAN): من القائمة المنسدلة تأمين الطبقة 2، حدد **802.1x**. بشكل افتراضي، يكون خيار تأمين الطبقة 2 هو **802.1x**. وهذا يمكن مصادقة **802.1x/EAP** للشبكة المحلية اللاسلكية (WLAN). تحت السياسات العامة، حدد مربع **تجاوز AAA**. عند تمكين تجاوز AAA، ولدى العميل معلمات مصادقة AAA ووحدة تحكم WLAN متعارضة، يتم إجراء مصادقة العميل بواسطة خادم AAA. حدد خادم RADIUS المناسب من القائمة المنسدلة تحت خوادم RADIUS. يمكن تعديل المعلمات الأخرى استناداً إلى متطلبات شبكة WLAN. **طبق**.

The screenshot displays the Cisco Systems WLAN configuration interface. The main navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'WLANs > Edit' page shows the following configuration details:

- WLAN ID:** 1
- WLAN SSID:** Admin
- General Policies:**
  - Radio Policy: All
  - Admin Status:  Enabled
  - Session Timeout (secs): 1800
  - Quality of Service (QoS): Silver (best effort)
  - WMM Policy: Disabled
  - 7920 Phone Support:  Client CAC Limit  AP CAC Limit
  - Broadcast SSID:  Enabled
  - Aironet IE:  Enabled
  - Allow AAA Override:  Enabled
  - Client Exclusion:  Enabled \*\* 60 (Timeout Value (secs))
  - DHCP Server:  Override
  - DHCP Addr. Assignment:  Required
  - Interface Name: management
  - MFP Version Required: 1
  - MFP Signature Generation:  (Global MFP Disabled)
  - H-REAP Local Switching:
- Security Policies:**
  - Layer 2 Security: 802.1X
  - MAC Filtering:
  - Layer 3 Security: None
  - Web Policy:
- Radius Servers:**
  - Server 1: IP:172.16.1.60, Port:1812 (Authentication Servers); none (Accounting Servers)

Red circles highlight the 'Apply' button, 'Admin Status', 'Aironet IE', 'Allow AAA Override', 'Client Exclusion', 'Layer 2 Security', and 'Server 1' configuration fields.

وبالمثل، لإنشاء شبكة محلية لاسلكية (WLAN) لقسم المبيعات، كرر الخطوات ب و ج. فيما يلي لقطات الشاشة.



Browser address bar: <https://172.16.1.30/screens/frz>

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > New

WLAN ID: 2  
WLAN SSID: Sales

< Back | Apply

Browser address bar: <https://172.16.1.30/screens/frz>

Cisco Systems | Save Configuration | Ping | Logout | Refresh

MONITOR | **WLANs** | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP

WLANs > Edit

WLAN ID: 2  
WLAN SSID: Sales

**General Policies**

Radio Policy: All  
Admin Status:  Enabled  
Session Timeout (secs): 1800  
Quality of Service (QoS): Silver (best effort)  
WMM Policy: Disabled  
7920 Phone Support:  Client CAC Limit  AP CAC Limit  
Broadcast SSID:  Enabled  
Aironet IE:  Enabled  
Allow AAA Override:  Enabled  
Client Exclusion:  Enabled \*\* 60  
Timeout Value (secs)  
DHCP Server:  Override  
DHCP Addr. Assignment:  Required  
Interface Name: management  
MFP Version Required: 1  
MFP Signature Generation:  (Global MFP Disabled)  
H-REAP Local Switching:   
\* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

**Security Policies**

Layer 2 Security: 802.1X  
 MAC Filtering  
Layer 3 Security: None  
 Web Policy \*

\*\* Web Policy cannot be used in combination with IPsec and L2TP.  
\*\* When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)  
\*\*\* CKIP is not supported by 10xx APs

**Radius Servers**

Authentication Servers | Accounting Servers

Server 1: IP:172.16.1.60, Port:1812 | none

## تكوين مصدر المحتوى الإضافي الآمن من Cisco

على خادم ACS الآمن من Cisco، يلزمك:

1. قم بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كعميل AAA.
  2. قم بإنشاء قاعدة بيانات المستخدم وحدد NAR للمصادقة المستندة إلى SSID.
  3. تمكين مصادقة EAP.
- أتمت هذا steps على ال Cisco ACS الآمن:

1. لتحديد وحدة التحكم كعميل AAA على خادم ACS، انقر فوق **تكوين الشبكة** من واجهة المستخدم الرسومية (ACS). ضمن AAA، انقر العملاء على إضافة إدخال.

The screenshot shows the Cisco Network Configuration web interface. On the left is a navigation menu with options like 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 content area is titled 'Network Configuration' and has a 'Select' dropdown menu. Below this, there are two main sections: 'AAA Clients' and 'AAA Servers'. The 'AAA Clients' section shows a table with columns 'AAA Client Hostname', 'AAA Client IP Address', and 'Authenticate Using', with the text 'None Defined' below it. The 'AAA Servers' section shows a table with columns 'AAA Server Name', 'AAA Server IP Address', and 'AAA Server Type', with one entry: 'tsweb-laptop', '127.0.0.1', and 'CiscoSecure ACS'. There are 'Add Entry' and 'Search' buttons for both sections, and a 'Back to Help' button at the bottom.

2. 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).

- 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

## Add AAA Client

AAA Client Hostname	<input type="text" value="WLC"/>
AAA Client IP Address	<input type="text" value="172.16.1.30"/>
Key	<input type="text" value="cisco123"/>
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	

Submit

Submit + Apply

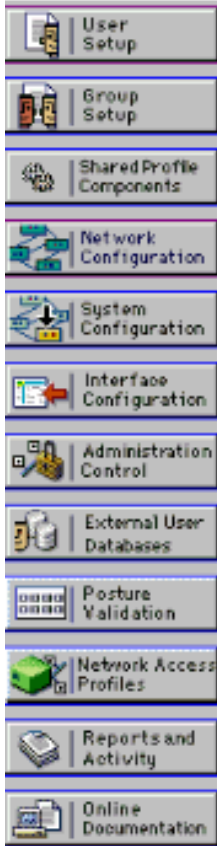
Cancel



Back to Help

3. طقطقت مستعمل **setup** من ال ACS gui، دخلت ال username، وطقطقة يضيف/يحرر. في هذا المثال، المستخدم هو A1.

4. عندما تظهر صفحة إعداد المستخدم، قم بتعريف كافة المعلمات الخاصة بالمستخدم. في هذا المثال، يتم تكوين اسم المستخدم وكلمة المرور ومعلومات المستخدم التكميلية لأنك تحتاج إلى هذه المعلمات لمصادقة LEAP.



User: A1 (New User)

Account Disabled

Supplementary User Info

Real Name: A1  
 Description: Admin Department User

User Setup

Password Authentication:

ACS Internal Database

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:

Submit Cancel

5. قم بالتمرير لأسفل في صفحة إعداد المستخدم، حتى ترى قسم فيود الوصول إلى الشبكة. تحت واجهة المستخدم لتقييد الوصول إلى DNIS/CLI، حدد الاتصال/ نقطة الوصول المسموح بها وحدد هذه المعلمات: **عمل AAA** — عنوان (172.16.1.30) IP WLC في المثال الذي ذكرناه) **المنفذ**—\*واجهة سطر الأوامر—\*ssidname\*—DNIS
6. تعرف سمة DNIS SSID المسموح للمستخدم بالوصول إليه. يرسل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) معرف SSID في سمة DNIS إلى خادم RADIUS. إذا كان المستخدم بحاجة إلى الوصول إلى مسؤول WLAN المسمى فقط، فأدخل **admin\*** لحقل DNIS. وهذا يضمن أن المستخدم لديه حق الوصول فقط إلى المسؤول المسمى بشبكة WLAN. **ملاحظة:** يجب دائما أن يسبق SSID \*. إنه إلزامي.

## Advanced Settings

-  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

### Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client: All AAA Clients

Port:  

Address:  

enter

---

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS

remove

AAA Client: WVLC

Port: \*

CLI: \*

DNIS: \*Admin

enter

Submit
Cancel

7. انقر على إرسال.

8. وبالمثل، قم بإنشاء مستخدم لمستخدم قسم المبيعات. هنا اللقطات.



# User Setup

Edit

- 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: S1 (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 caching is enabled.

Group to which the user is assigned:

- 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

### Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client All AAA Clients

Port  

Address  

enter

---

Define CLI/DNIS-based access restrictions

Table Defines : Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS

remove

AAA Client WLC

Port \*

CLI \*

DNIS \*Sales

enter

Submit
Cancel

9. كرر نفس العملية لإضافة المزيد من المستخدمين إلى قاعدة البيانات. **ملاحظة:** يتم تجميع جميع المستخدمين بشكل افتراضي ضمن المجموعة الافتراضية. إذا كنت تريد تعيين مستخدمين محددین لمجموعات مختلفة، ارجع إلى قسم [إدارة مجموعة المستخدمين في دليل المستخدم لـ Cisco Secure ACS لـ Windows Server](#) **3.2. ملاحظة:** إذا لم يظهر لديك قسم "قيود الوصول إلى الشبكة" في نافذة "إعداد المستخدم"، فقد يكون السبب هو عدم تمكنه. لتمكين تقييدات الوصول إلى الشبكة للمستخدمين، اختر واجهات < خيارات متقدمة من واجهة المستخدم الرسومية (ACS)، وحدد تقييدات الوصول إلى الشبكة على مستوى المستخدم وانقر فوق إرسال. يتيح ذلك NAR ويظهر في نافذة إعداد المستخدم.



# Interface Configuration

Edit

- 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

## Advanced Options

**Note: Only the selected options will appear in the user interface.**













- Per-user TACACS+/RADIUS Attributes
- User-Level Shared Network Access Restrictions
- User-Level Network Access Restrictions
- User-Level Downloadable ACLs
- Default Time-of-Day / Day-of-Week Specification
- Group-Level Shared Network Access Restrictions
- Group-Level Network Access Restrictions
- Group-Level Downloadable ACLs
- Group-Level Password Aging
- Network Access Filtering
- Max Sessions
- Usage Quotas
- Distributed System Settings
- Remote Logging
- ACS internal database Replication
- RDBMS Synchronization
- IP Pools
- Network Device Groups
- Voice-over-IP (VoIP) Group Settings
- Voice-over-IP (VoIP) Accounting Configuration
- ODBC Logging

Submit

Cancel



## Advanced Settings

-  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

### Network Access Restrictions (NAR) ?

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client: All AAA Clients

Port:

Address:

enter

---

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS

remove

AAA Client: WVLC

Port:

CLI:

DNIS:

enter

Submit
Cancel

10. لتمكين مصادقة EAP، انقر على **تكوين النظام وإعداد المصادقة العامة** لضمان تكوين خادم المصادقة لتنفيذ أسلوب مصادقة EAP المطلوب. تحت إعدادات تكوين EAP حدد أسلوب EAP المناسب. يستخدم هذا المثال مصادقة LEAP. انقر فوق إرسال عند الانتهاء.

- 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

## Global Authentication Setup

EAP Configuration ?

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Allow Posture Validation

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

[EAP-FAST Configuration](#)

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

---

**LEAP**

Allow LEAP (For Aironet only)

---

**EAP-MD5**

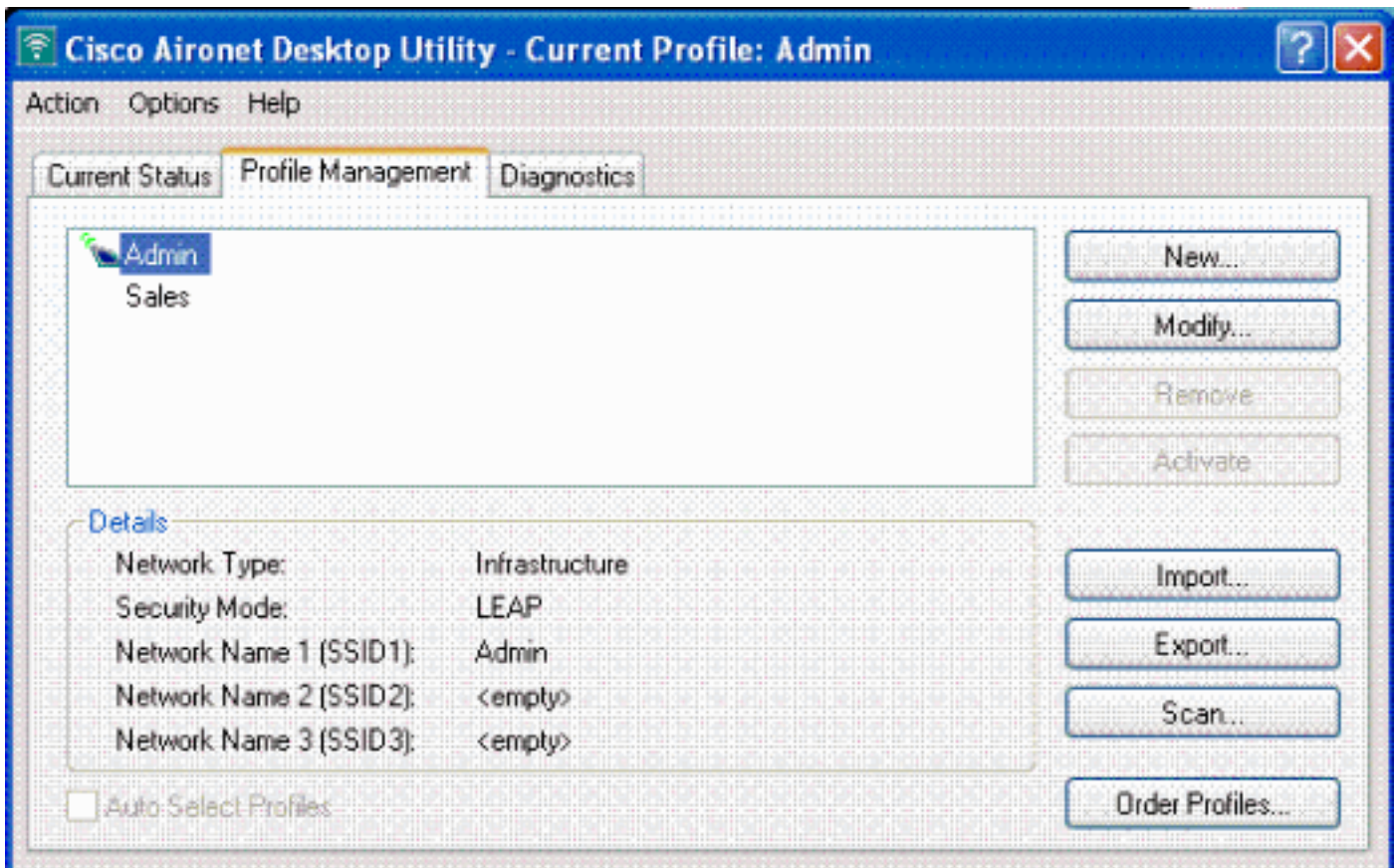
Submit
Submit + Restart
Cancel

## تكوين العميل اللاسلكي والتحقق

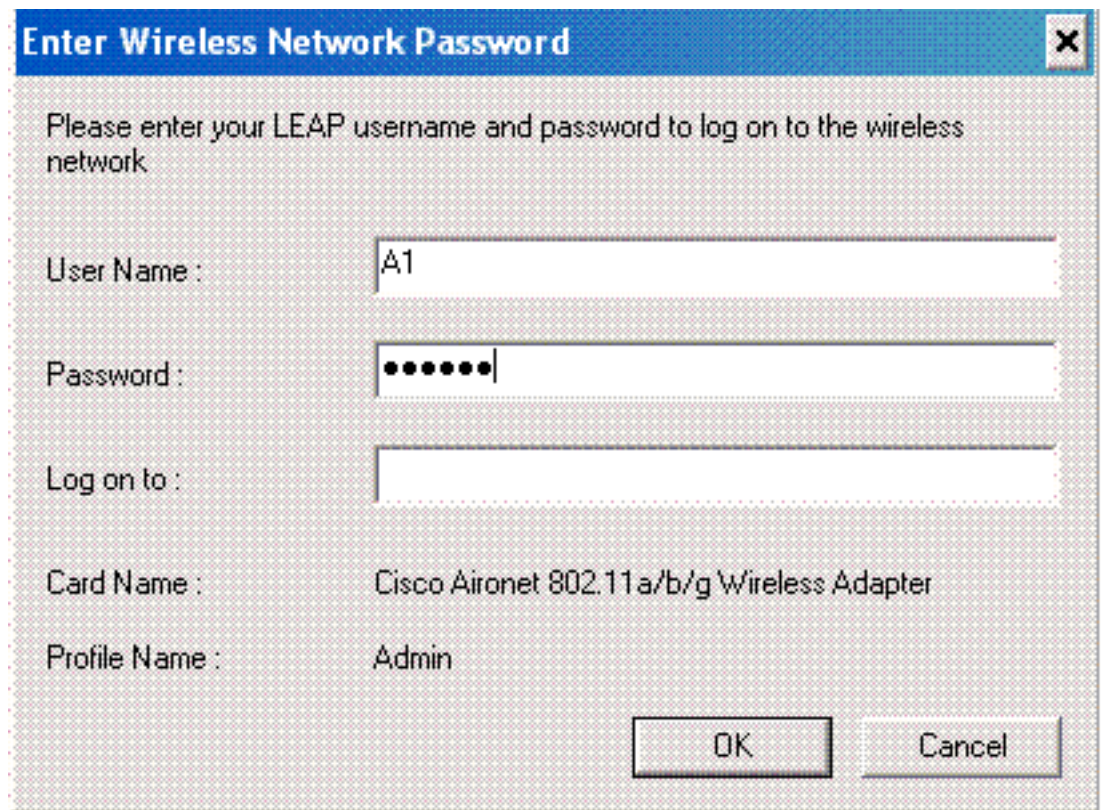
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح. حاول إقران عميل لاسلكي بنقطة الوصول في الوضع Lightweight باستخدام مصادقة LEAP للتحقق من عمل التكوين كما هو متوقع.

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

**ملاحظة:** من وحدة المعالجة المركزية (ADU)، ترى أنك قمت بتكوين توصيفي عميل. واحد لمستخدمي قسم الإدارة مع إدارة SSID والآخر لمستخدمي قسم المبيعات مع مبيعات SSID. يتم تكوين كلا التوصيفين لمصادقة LEAP.



عند تنشيط توصيف المستخدم اللاسلكي من قسم الإدارة، يطلب من المستخدم توفير اسم المستخدم/كلمة المرور لمصادقة LEAP. فيما يلي مثال:

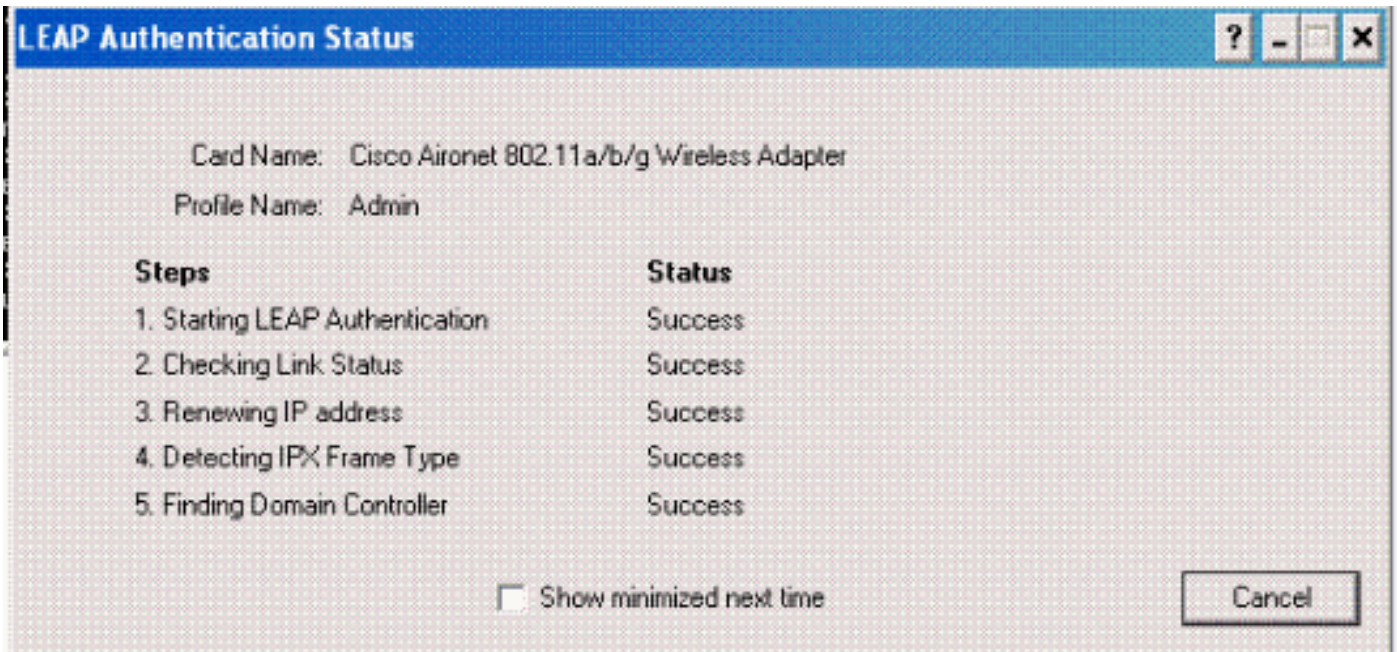


تمرر نقاط الوصول في الوضع Lightweight ثم ال WLC على مسوغات المستخدم إلى خادم RADIUS الخارجي (Cisco Secure ACS) للتحقق من المسوغات. يمرر عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بيانات الاعتماد بما في ذلك سمة DNIS (اسم SSID) إلى خادم RADIUS للتحقق.

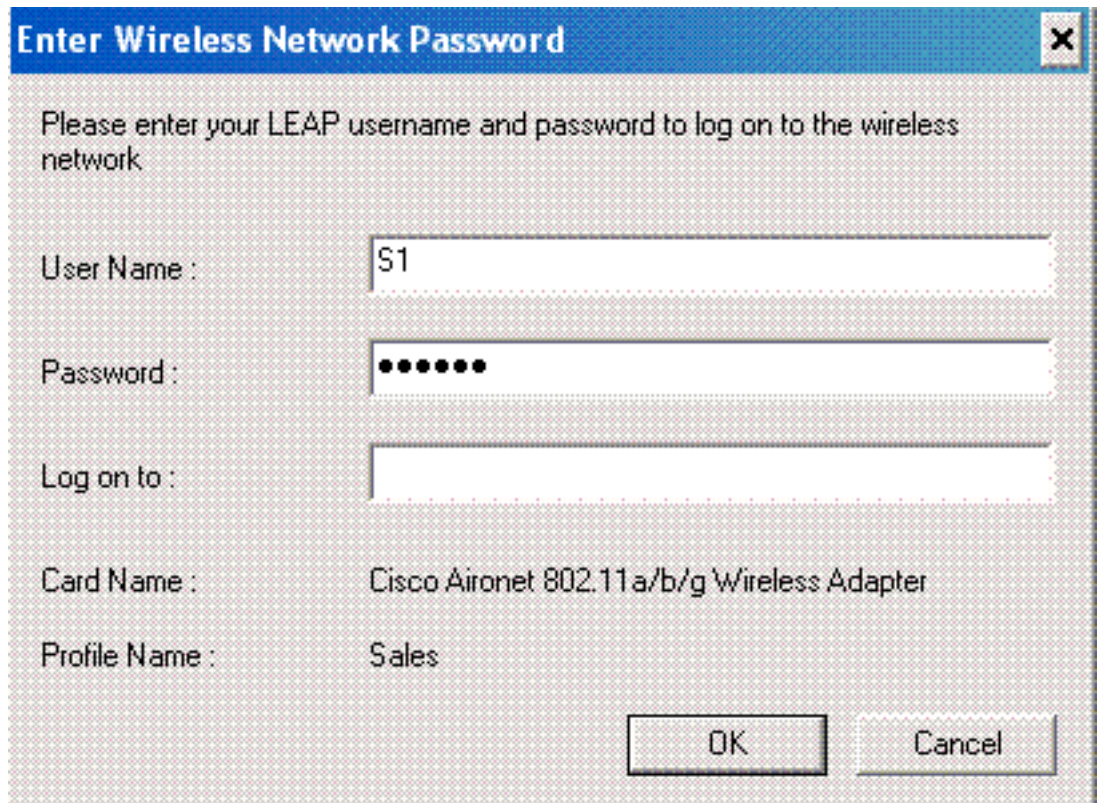
يتحقق خادم RADIUS من مسوغات المستخدم بمقارنة البيانات بقاعدة بيانات المستخدم (وأوراق NAR)، ويوفر

الوصول إلى العميل اللاسلكي كلما كانت مسوغات المستخدم صالحة.

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



وبالمثل، عندما يقوم مستخدم من قسم المبيعات بتنشيط ملف تعريف المبيعات، تتم مصادقة المستخدم بواسطة خادم RADIUS استنادا إلى اسم مستخدم/كلمة مرور LEAP و SSID.



يظهر تقرير المصادقة الذي تم تمريره على خادم ACS أن العميل قد اجتاز مصادقة RADIUS (مصادقة EAP ومصادقة SSID). فيما يلي مثال:

## Reports and Activity

Select

Passed Authentications active.csv Refresh Download

Regular Expression Start Date & Time End Date & Time Rows per Page

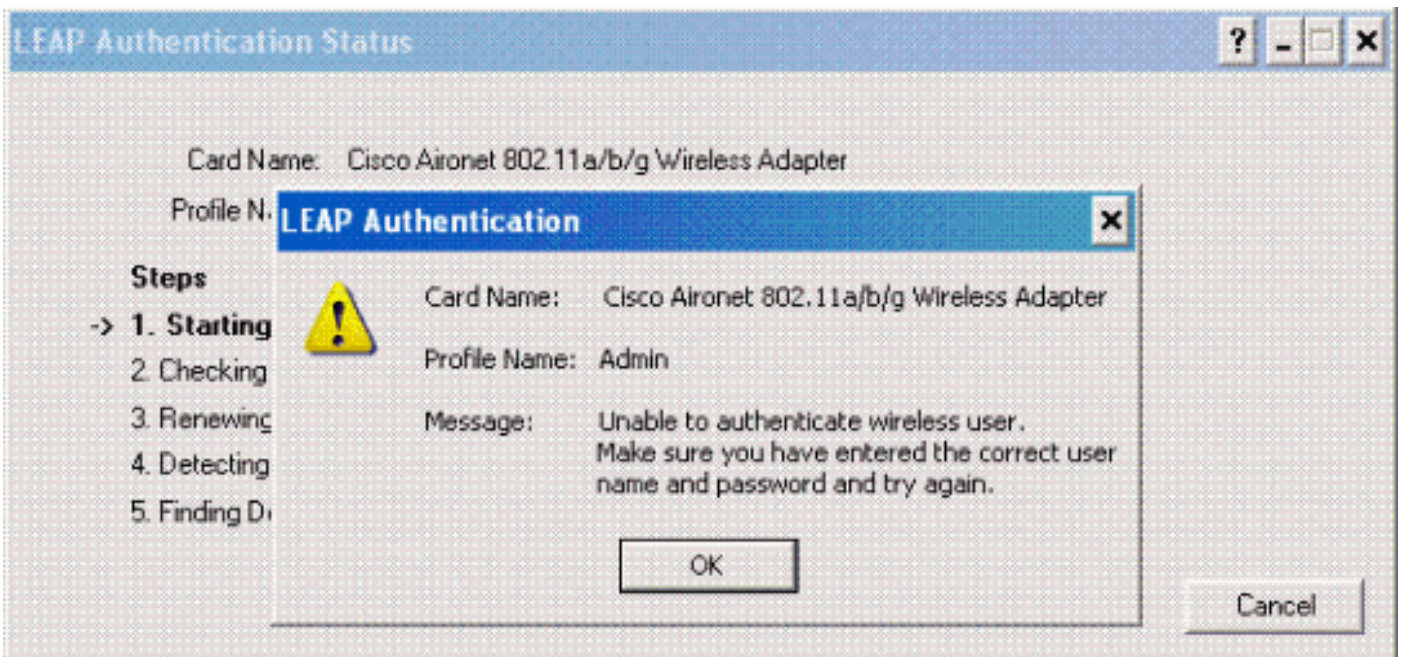
mm/dd/yyyy, hh:mm:ss mm/dd/yyyy, hh:mm:ss 50

Apply Filter Clear Filter

Filtering is not applied.

Date	Time	Message-Type	User-Name	Group-Name	Caller-ID	NAR-Port	NAS-IP-Address	Network Access Profile Name	Shared BAC	Downloadable ACL	System-Posture-Token	Application-Posture-Token	Reason	EAP Type	EAP Type Name
10/11/2006	14:48:40	Authen OK	S1	Default Group	00-40-9E-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP
10/11/2006	14:47:05	Authen OK	A1	Default Group	00-40-9E-57	1	172.16.1.30	(Default)	..	..	..	..	..	17	LEAP

الآن، إذا حاول مستخدم المبيعات الوصول إلى SSID المسؤول، يرفض خادم RADIUS وصول المستخدم إلى شبكة WLAN. فيما يلي مثال:



بهذه الطريقة يمكن تقييد وصول المستخدمين بناء على SSID. في بيئة المؤسسة، يمكن تجميع جميع المستخدمين الذين يقعون في قسم معين في مجموعة واحدة ويمكن توفير الوصول إلى شبكة WLAN استناداً إلى SSID الذي يستخدمونه كما هو موضح في هذا المستند.

## استكشاف الأخطاء وإصلاحها

### أوامر استكشاف الأخطاء وإصلاحها

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر `show`. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر `show`.

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

- `debug dot1x aaa enable`—يمكن تصحيح أخطاء تفاعلات 802.1x AAA
- `debug dot1x enable` ربط—يمكن ال debug من كل ربط dot1x
- `debug aaa all enable`—يشكل تصحيح أخطاء جميع رسائل AAA

يمكنك أيضا استخدام تقرير المصادقة الذي تم تمريره وتقرير المصادقة الفاشل على خادم Cisco Secure ACS لاستكشاف أخطاء التكوين وإصلاحها. وتدرج هذه التقارير ضمن نافذة التقارير والأنشطة على واجهة المستخدم الرسومية (ACS).

## معلومات ذات صلة

- [مصادقة EAP باستخدام مثال تكوين وحدات التحكم في الشبكة المحلية اللاسلكية \(WLC\)](#)
- [مثال تكوين مصادقة الويب لوحدة تحكم الشبكة المحلية \(LAN\) اللاسلكية](#)
- [مجموعة AP VLANs مع لاسلكي lan جهاز تحكم تشكيل مثال](#)
- [صفحة الدعم اللاسلكي](#)
- [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 ة 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