

# EAP-FAST عم Cisco Secure Services Client

## المحتويات

<a href="#">المقدمة</a>
<a href="#">المتطلبات الأساسية</a>
<a href="#">المتطلبات</a>
<a href="#">المكونات المستخدمة</a>
<a href="#">الاصطلاحات</a>
<a href="#">محددات التصميم</a>
<a href="#">قاعدة البيانات</a>
<a href="#">تشفير</a>
<a href="#">تسجيل دخول أحادي وبيانات اعتماد الجهاز</a>
<a href="#">الرسم التخطيطي للشبكة</a>
<a href="#">تكوين خادم التحكم في الوصول (ACS)</a>
<a href="#">إضافة نقطة وصول كعميل (AAA) في ACS</a>
<a href="#">تكوين ACS للاستعلام عن قاعدة البيانات الخارجية</a>
<a href="#">تمكين دعم EAP-FAST على ACS</a>
<a href="#">وحدة التحكم في شبكة WLAN من Cisco</a>
<a href="#">تكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية</a>
<a href="#">التشغيل الأساسي وتسجيل نقاط الوصول في الوضع Lightweight لوحدة التحكم</a>
<a href="#">مصادقة RADIUS من خلال ACS الآمن من Cisco</a>
<a href="#">تكوين معلمات WLAN</a>
<a href="#">التحقق من العملية</a>
<a href="#">الملحق</a>
<a href="#">التقاط EAP-FAST Exchange J sniffer</a>
<a href="#">تصحيح الأخطاء في وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN)</a>
<a href="#">معلومات ذات صلة</a>

## المقدمة

يصف هذا المستند كيفية تكوين Cisco Secure Services Client (CSSC) باستخدام وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية وبرنامج Microsoft Windows 2000<sup>®</sup> وبرنامج Cisco Secure Access Control Server (ACS) 4.0 من خلال EAP-FAST. يقدم هذا المستند بنية EAP-FAST ويقدم أمثلة على النشر والتكوين. CSSC هو مكون برنامج العميل الذي يوفر اتصال بيانات اعتماد المستخدم بالبنية الأساسية لمصادقة مستخدم على الشبكة وتخصيص الوصول المناسب.

هذه بعض ميزات حل CSSC كما هو موضح في هذا المستند:

- مصادقة كل مستخدم (أو جهاز) قبل الوصول إلى إذن الشبكة المحلية اللاسلكية (WLAN)/الشبكة المحلية اللاسلكية (LAN) مع بروتوكول المصادقة المتوسع (EAP)

- حل أمان شامل لشبكة WLAN مع مكونات الخادم والمصادقة والعميل
  - حل مشترك للمصادقة السلكية واللاسلكية
  - مفاتيح تشفير ديناميكية لكل مستخدم مشتقة في عملية المصادقة
  - لا يتطلب وجود بنية أساسية للمفتاح العام (PKI) أو شهادات (التحقق من الشهادة إختياري)
  - الوصول إلى إطار عمل EAP الذي تم تمكينه ل NAC و/أو
- ملاحظة: ارجع إلى [مخطط Cisco Safe اللاسلكي](#) للحصول على معلومات حول نشر الاتصال اللاسلكي الآمن.

تم دمج إطار مصادقة 802.1x كجزء من معيار 802.11i (أمان الشبكة المحلية اللاسلكية) لتمكين وظائف المصادقة والتفويض والمحاسبة المستندة إلى الطبقة 2 في شبكة شبكة محلية لاسلكية 802.11. توجد اليوم العديد من بروتوكولات EAP المتاحة للنشر في كل من الشبكات السلكية واللاسلكية. تتضمن بروتوكولات EAP المنشورة بشكل شائع LEAP و PEAP و EAP-TLS. وبالإضافة إلى هذه البروتوكولات، قامت Cisco بتعريف وتنفيذ مصادقة EAP المرنة من خلال بروتوكول النفق الآمن (EAP-FAST) كبروتوكول EAP قائم على المعايير متاح للنشر في شبكات LAN السلكية واللاسلكية على حد سواء. تتوافر مواصفات بروتوكول EAP-FAST للجمهور على [موقع IETF على الويب](#).

كما هو الحال مع بعض بروتوكولات EAP الأخرى، فإن EAP-FAST هو بنية أمان العميل-الخادم التي تقوم بتشغيل حركات EAP داخل نفق TLS. وعلى الرغم من التشابه مع PEAP أو EAP-TTLS في هذا الصدد، فإنه يختلف في أن إنشاء نفق EAP-FAST يقوم على مفاتيح سرية مشتركة قوية تكون فريدة لكل مستخدم في مقابل PEAP/EAP-TTLS (التي تستخدم شهادة خادم X.509 لحماية جلسة المصادقة). وتسمى هذه المفاتيح السرية المشتركة بيانات اعتماد الوصول المحمي (PACs) ويمكن توزيعها تلقائياً (الإمداد التلقائي أو داخل النطاق الترددي) أو يدوياً (الإمداد اليدوي أو خارج النطاق الترددي) على أجهزة العميل. ولأن المصادقة التي تعتمد على الأسرار المشتركة أكثر فعالية من المصادقة التي تعتمد على البنية الأساسية PKI، فإن EAP-FAST هو أسرع أنواع EAP التي تعتمد على المعالج بشكل أقل والتي توفر عمليات تبادل للمصادقة المحمية. كما أن EAP-FAST مصمم لضمان بساطة النشر لأنه لا يتطلب شهادة على عميل الشبكة المحلية اللاسلكية أو على البنية الأساسية RADIUS ومع ذلك فإنه يتضمن آلية إمداد مدمجة.

وهذه بعض القدرات الرئيسية لبروتوكول EAP-FAST:

- تسجيل دخول أحادي (SSO) باستخدام اسم مستخدم/كلمة مرور Windows
- دعم تنفيذ البرنامج النصي لتسجيل الدخول
- دعم وصول Wi-Fi المحمي (WPA) دون مطالبة من جهة خارجية (Windows 2000 و XP فقط)
- عملية نشر بسيطة دون الحاجة لبنية PKI الأساسية
- شيخوخة كلمة مرور Windows (أي دعم انتهاء صلاحية كلمة المرور المستندة إلى الخادم)
- التكامل مع Cisco Trust Agent للتحكم في الدخول إلى الشبكة مع برامج العميل المناسبة

## المتطلبات الأساسية

### المتطلبات

هناك افتراض بأن الميث لديه معرفة بشييت Windows 2003 الأساسي وشييت Cisco WLC حيث أن هذا المستند يغطي فقط المكونات المحددة لتسهيل الاختبارات.

للحصول على معلومات الشبيت الأولى ومعلومات التكوين لوحات التحكم من السلسلة Cisco 4400 Series، ارجع إلى [دليل البدء السريع: وحدات التحكم في الشبكة المحلية اللاسلكية من السلسلة Cisco 4400 Series](#). للحصول على معلومات الشبيت الأولى ومعلومات التكوين لوحات التحكم من السلسلة Cisco 2000 Series، ارجع إلى [دليل البدء السريع: سلسلة وحدات التحكم في الشبكة المحلية اللاسلكية Cisco 2000 Series](#).

قبل البدء، قم بشييت Microsoft Windows Server 2000 باستخدام أحدث برنامج لحزمة الخدمة. قم بشييت وحدات التحكم ونقاط الوصول في الوضع Lightweight (نقاط الوصول في الوضع Lightweight (LAPs) وتأكد من تكوين آخر تحديثات البرامج.

## المكونات المستخدمة

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

- وحدة التحكم من السلسلة Cisco 2006 أو Series 4400 التي تشغل الإصدار 4.0.155.5
- cisco 1242 LWAPP AP
- Windows 2000 مع Active Directory
- cisco مادة حفازة 3750G مفتاح
- Windows XP مع بطاقة مهايي CB21AG و Cisco Secure Services Client، الإصدار 4.05

## الاصطلاحات

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

## محددات التصميم

### قاعدة البيانات

عند نشر شبكة WLAN والسعي إلى بروتوكول مصادقة، من المرغوب بشكل عام استخدام قاعدة بيانات حالية لمصادقة المستخدم/الجهاز. قواعد البيانات النموذجية التي يمكن استخدامها هي Windows Active Directory أو LDAP أو قاعدة بيانات كلمة مرور الواحدة (OTP) (أي RSA أو SecureID). جميع قواعد البيانات هذه متوافقة مع بروتوكول EAP-FAST، ولكن عندما تخطط للنشر، هناك بعض متطلبات التوافق التي يجب مراعاتها. يتم تحقيق النشر الأولي لملف مسوغات الوصول المحمي (PAC) إلى العملاء من خلال التوفير التلقائي المجهول أو الإمداد المصادق (من خلال شهادة العميل الحالي X.509) أو الإمداد اليدوي. لأغراض هذا المستند، يتم مراعاة التوفير التلقائي للمجهول والإمداد اليدوي.

يستخدم إمداد PAC التلقائي بروتوكول إتفاقية مفتاح (ADHP Diffie-Hellman) المصادق لإنشاء نفق آمن. يمكن إنشاء النفق الآمن إما بشكل مجهول أو من خلال آلية مصادقة الخادم. ضمن اتصال النفق المنشأ، يستخدم MS-CHAPv2 لمصادقة العميل، وعند المصادقة الناجحة، لتوزيع ملف مسوغ الوصول المحمي إلى العميل. بعد توفير مسوغ الوصول المحمي (PAC) بنجاح، يمكن استخدام ملف مسوغات الوصول المحمي (PAC) لبدء جلسة مصادقة جديدة EAP-FAST للحصول على وصول آمن إلى الشبكة.

إن توفير مسوغ الوصول المحمي التلقائي مرتبط بقاعدة البيانات المستخدمة لأنه، نظرا لأن آلية الإمداد التلقائي تعتمد على MSCHAPv2، فإن قاعدة البيانات المستخدمة للمصادقة على المستخدمين يجب أن تكون متوافقة مع تنسيق كلمة المرور هذا. إذا كنت تستخدم EAP-FAST مع قاعدة بيانات لا تدعم تنسيق MSCHAPv2 (مثل OTP أو Novell أو LDAP)، فإنه يتطلب استخدام آلية أخرى (أي الإمداد اليدوي أو الإمداد المصدق) لنشر ملفات مسوغات الوصول المحمي الخاصة بالمستخدم. يعطى هذا المستند مثلا للتوفير التلقائي باستخدام قاعدة بيانات مستخدم Windows.

### تشفير

لا تتطلب مصادقة EAP-FAST استخدام نوع تشفير WLAN محدد. يتم تحديد نوع تشفير WLAN الذي سيتم استخدامه بواسطة إمكانات بطاقة واجهة الشبكة (NIC) الخاصة بالعميل. يوصى باستخدام تشفير AES-WPA2 (CCM أو WPA(TKIP))، حسب إمكانات بطاقة واجهة الشبكة (NIC) في عملية نشر محددة. لاحظ أن حل Cisco WLAN يسمح بوجود كلا من WPA2 وأجهزة عميل WPA على SSID مشترك.

إذا كانت أجهزة العميل لا تدعم WPA2 أو WPA، فمن الممكن نشر مصادقة 802.1X باستخدام مفاتيح WEP الديناميكية، ولكن نظرا للمستكشفات المعروفة مقابل مفاتيح WEP، لا يوصى بآلية تشفير WLAN هذه. إذا كان من المطلوب دعم عملاء WEP فقط، يوصى باستخدام فاصل زمني بين جلسة ومهلة، مما يتطلب أن يستخرج العملاء مفتاح WEP جديد على فاصل زمني متكرر. ثلاثين دقيقة هي فترة جلسة العمل الموصى بها لمعدلات بيانات شبكة WLAN النموذجية.

## تسجيل دخول أحادي وبيانات اعتماد الجهاز

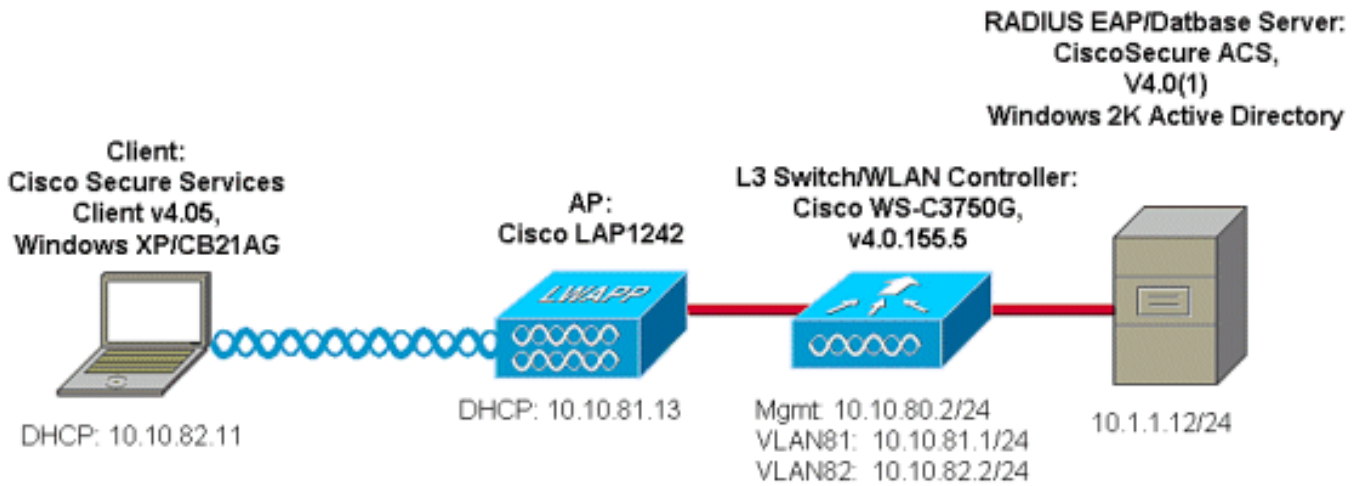
يشير تسجيل الدخول الأحادي إلى قدرة تسجيل دخول مستخدم واحد أو إدخال بيانات اعتماد المصادقة المراد استخدامها للوصول إلى تطبيقات متعددة أو أجهزة متعددة. لأغراض هذا المستند، يشير تسجيل الدخول الأحادي إلى استخدام بيانات الاعتماد المستخدمة لتسجيل الدخول إلى جهاز كمبيوتر للمصادقة على شبكة WLAN.

باستخدام Cisco Secure Services Client، من الممكن استخدام بيانات اعتماد تسجيل الدخول الخاصة بمستخدم للمصادقة أيضا على شبكة WLAN. في حالة الرغبة في مصادقة جهاز كمبيوتر إلى الشبكة قبل تسجيل دخول المستخدم إلى الكمبيوتر، يلزم استخدام بيانات اعتماد المستخدم المخزنة أو بيانات الاعتماد المرتبطة بملف تعريف الجهاز. وبعد أي من هذه الأساليب مفيدا في الحالات التي يكون فيها تشغيل البرامج النصية لتسجيل الدخول أو تعيين محركات الأقراص عند تمهيد الكمبيوتر، وذلك على العكس من الحالات التي يقوم فيها المستخدم بتسجيل الدخول.

## الرسم التخطيطي للشبكة

هذا هو الرسم التخطيطي للشبكة المستخدم في هذا المستند. في هذه الشبكة، هناك أربع شبكات فرعية مستخدمة. لاحظ أنه من غير الضروري تقسيم هذه الأجهزة إلى شبكات مختلفة، ولكن هذا يوفر أقصى قدر من المرونة للدمج مع الشبكات الفعلية. توفر وحدة التحكم في الشبكة المحلية اللاسلكية المدمجة Catalyst 3750G إمكانات محولات التزويد بالطاقة عبر شبكة إيثرنت (POE) والتحويل من المستوى الثالث ووحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) على هيكل مشترك.

1. الشبكة 10.1.1.0 هي شبكة الخادم التي يتواجد فيها ACS.
2. الشبكة 10.10.80.0 هي شبكة الإدارة المستخدمة بواسطة وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN).
3. الشبكة 10.10.81.0 هي الشبكة التي توجد بها نقاط الوصول.
4. يتم استخدام الشبكة 10.10.82.0 لعملاء شبكة WLAN.



## تكوين خادم التحكم في الوصول (ACS)

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.

## إضافة نقطة وصول كعميل (AAA) في ACS

يصف هذا القسم كيفية تكوين ACS ل EAP-FAST مع توفير PAC داخل النطاق مع Windows Active Directory كقاعدة بيانات خارجية.

1. قم بتسجيل الدخول إلى ACS < تكوين الشبكة وانقر فوق إضافة إدخال.
2. قم بتعبئة اسم وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) وعنوان IP والمفتاح السري المشترك وتحت "المصادقة باستخدام"، اختر RADIUS (Cisco Airespace)، والذي يتضمن أيضا سمات RADIUS IETF. ملاحظة: في حالة تمكين مجموعات أجهزة الشبكة (NDG)، اختر أولا NDG المناسب وقم بإضافة وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) إليها. ارجع إلى دليل تكوين ACS للحصول على تفاصيل حول NDG.
3. انقر على إرسال+ إعادة تشغيل.

**CISCO SYSTEMS** Network Configuration

**Edit**

### AAA Client Setup For ws-3750

AAA Client IP Address: 10.10.80.3

Key: cisco123

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

Submit Submit + Apply Delete Delete + Apply Cancel

Back to Help

## تكوين ACS للاستعلام عن قاعدة البيانات الخارجية

يصف هذا القسم كيفية تكوين ACS للاستعلام عن قاعدة البيانات الخارجية.

1. طقطقت خارجي مستعمل قاعدة معطيات < قاعدة معطيات تشكيل < Windows قاعدة معطيات < بشكل.
2. تحت تكوين قائمة المجالات، قم بنقل المجالات من المجالات المتاحة إلى قائمة المجالات. ملاحظة: يجب أن يكون لدى الخادم الذي يشغل ACS معرفة بهذه المجالات من أجل تطبيق ACS للكشف عن هذه المجالات واستخدامها لأغراض المصادقة.



## External User Databases

- 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

If the unknown user policy contains additional external databases and the Windows database is not the last database on the Selected Databases list, you may enable this option.

### Configure Domain List

Available Domains	Domain List
	TME

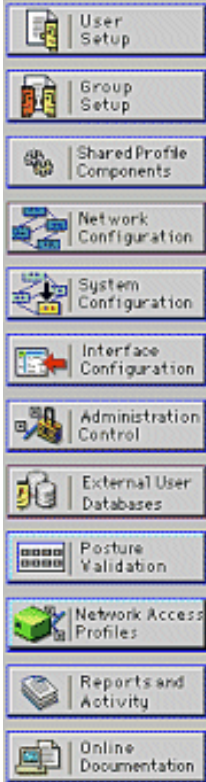
->  
<-

Up Down

3. تحت إعدادات Windows EAP، قم بتكوين الخيار للسماح بتغيير كلمة المرور داخل PEAP أو EAP-FAST جلسة. ارجع إلى [دليل التكوين ل Cisco Secure ACS 4.1](#) للحصول على مزيد من التفاصيل حول EAP-FAST وكلمة مرور Windows.

4. انقر على إرسال. ملاحظة: يمكنك أيضا تمكين ميزة "إذن الطلب الهاتفي" ل EAP-FAST ضمن "تكوين قاعدة بيانات مستخدم Windows" للسماح لقاعدة بيانات Windows الخارجية بالتحكم في إذن الوصول. لا تنطبق إعدادات MS-CHAP لتغيير كلمة المرور في صفحة تكوين قاعدة بيانات Windows إلا على مصادقة MS-CHAP غير EAP. لتمكين تغيير كلمة المرور بالاقتران مع EAP-FAST، من الضروري تمكين تغيير كلمة المرور ضمن إعدادات Windows EAP.





### Windows EAP Settings ?

Enable password change inside PEAP or EAP-FAST.  
 EAP-TLS Strip Domain Name.

---

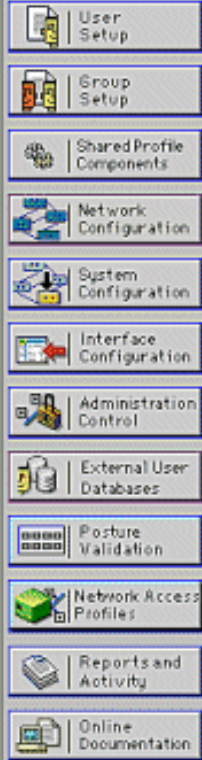
**Machine Authentication.**

Enable PEAP machine authentication.  
 Enable EAP-TLS machine authentication.  
 EAP-TLS and PEAP machine authentication name prefix:   
 Enable machine access restrictions.  
 Aging time (hours):   
 Group map for successful user authentication without machine authentication:   
 User Groups that are exempt from passing machine authentication:

Available User Groups		Selected User Groups
Default Group	->	
Group 1		
Group 2	->	
Group 3		
Group 4	->	
Group 5		
Group 6	->	
Group 7		
Group 8	->	

These settings can be used to enable or disable specific Windows EAP functionality

5. انقر على قاعدة بيانات المستخدم الخارجي < سياسة مستخدم غير معروفة واختر زر التحقق من قواعد بيانات المستخدم الخارجية التالية.
6. نقل قاعدة بيانات Windows من قواعد البيانات الخارجية إلى قواعد البيانات المحددة.
7. انقر على إرسال. ملاحظة: من هذه النقطة فصاعدا، يتحقق ACS من قاعدة بيانات Windows. إذا لم يتم العثور على المستخدم في قاعدة البيانات المحلية ل ACS، فإنه يضع المستخدم في مجموعة ACS الافتراضية. ارجع إلى وثائق ACS للحصول على مزيد من التفاصيل حول تعيينات مجموعة قواعد البيانات. ملاحظة: مع استعلامات ACS لقاعدة بيانات Microsoft Active Directory للتحقق من بيانات اعتماد المستخدم، يلزم تكوين إعدادات إضافية لحقوق الوصول على Windows. ارجع إلى دليل التثبيت ل Cisco Secure ACS ل Windows Server للحصول على تفاصيل.



### Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the ACS Internal Database.

Fail the attempt  
 Check the following external user databases

External Databases	Selected Databases
	Windows Database(Wind...

### Configure Enable Password Behaviour

For newly created dynamic users, the TACACS+ enable password is authenticated against:

The internal database.  
 The database in which the user profile is held.

## تمكين دعم EAP-FAST على ACS

يوضح هذا القسم كيفية تمكين دعم EAP-FAST على ACS.

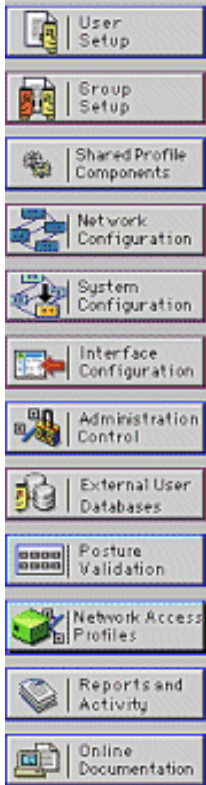
1. انتقل إلى تكوين النظام < إعداد المصادقة العامة > تكوين EAP-FAST.
2. أختار السماح ب EAP-FAST.
3. قم بتكوين هذه التوصيات: المفتاح الرئيسي TTL / المفتاح الرئيسي المتقاعد TTL / PAC TTL. يتم تكوين هذه الإعدادات بشكل افتراضي في ACS الآمن من Cisco: مفتاح رئيسي 1:TTL شهرمفتاح TTL المتقاعد: 3 أشهرPAC TTL: أسبوع واحد
4. املأ حقل معلومات معرف السلطة. يظهر هذا النص في بعض برامج عميل EAP-FAST حيث يكون تحديد مرجع مسوغات الوصول المحمي هو وحدة التحكم. ملاحظة: لا يستخدم عميل Cisco Secure Services هذا النص الوصفي لسلطة مسوغات الوصول المحمي (PAC).
5. أختار حقل السماح بإمداد مسوغ الوصول المحمي داخل النطاق. يتيح هذا الحقل إمداد مسوغات الوصول المحمي تلقائياً لعملاء EAP-FAST الذين تم تمكينهم بشكل صحيح. على سبيل المثال، يتم استخدام الإمداد التلقائي.
6. أختار الأساليب الداخلية المسموح بها: EAP-GTC و EAP-MSCHAP2. وهذا يسمح بتشغيل كل من عملاء EAP-FAST v1 و EAP-FAST v1a. (يدعم Cisco Secure Services Client EAP-FAST v1a). إذا لم يكن من الضروري دعم عملاء EAP-FAST v1، فلا يلزم إلا تمكين EAP-MSCHAPv2 كطريقة داخلية.
7. أختار خانة الاختيار EAP-FAST Master Server لتمكين خادم EAP-FAST هذا كخادم أساسي. وهذا يسمح لخوادم ACS الأخرى باستخدام هذا الخادم كمرجع PAC الرئيسي لتجنب توفير مفاتيح فريدة لكل ACS في الشبكة. ارجع إلى دليل تكوين ACS للحصول على التفاصيل.





## System Configuration

### EAP-FAST Configuration



#### EAP-FAST Settings

**EAP-FAST**

Allow EAP-FAST

Active master key TTL: 1 months

Retired master key TTL: 3 months

Tunnel PAC TTL: 1 weeks

Client initial message: TME

Authority ID Info: TME

Allow anonymous in-band PAC provisioning

Allow authenticated in-band PAC provisioning

Accept client on authenticated provisioning

Require client certificate for provisioning

Allow Machine Authentication

Machine PAC TTL: 1 weeks

Allow Stateless session resume

Authorization PAC TTL: 1 hours

Allowed inner methods:

EAP-GTC

EAP-MSCHAPv2

EAP-TLS

Select one or more of the following EAP-TLS comparison methods:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes): 120

EAP-FAST master server

Actual EAP-FAST server status: Master

### وحدة التحكم في شبكة WLAN من Cisco

لأغراض دليل النشر هذا، يتم استخدام وحدة التحكم في الشبكة المحلية اللاسلكية المدمجة (WLC) من Cisco WS3750G مع نقاط الوصول في الوضع (Lightweight) LAP من Cisco AP1240 لتوفير البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) لاختبارات CSSC. التشكيل مناسب لأي وحدة تحكم في الشبكة المحلية اللاسلكية (WLAN) من Cisco. إصدار البرنامج المستخدم هو 4.0.155.5.

### تكوين وحدة التحكم في الشبكة المحلية (LAN) اللاسلكية

### التشغيل الأساسي وتسجيل نقاط الوصول في الوضع Lightweight لوحدة 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 إستخدام 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 في معالج تكوين بدء التشغيل. أستخدم معالج التكوين لتكوين الإعدادات الأساسية. يمكنك الوصول إلى المعالج من خلال واجهة سطر الأوامر (CLI) أو واجهة المستخدم الرسومية (GUI). 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]: ws-3750
Enter Administrative User Name (24 characters max): admin
***** : (Enter Administrative Password (24 characters max
Management Interface IP Address: 10.10.80.3
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.10.80.2
:(Management Interface VLAN Identifier (0 = untagged
Management Interface DHCP Server IP Address: 10.10.80.2
AP Manager Interface IP Address: 10.10.80.4
AP-Manager is on Management subnet, using same values
:(AP Manager Interface DHCP Server (172.16.1.1
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: Security
Network Name (SSID): Enterprise
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 (WLC) كعنوان IP لواجهة الإدارة 10.10.80.4 و كعنوان IP لواجهة AP-Manager.

قبل تكوين أي ميزات أخرى على قوائم التحكم في الشبكة المحلية اللاسلكية (WLCs)، يجب تسجيل نقاط الوصول في الوضع Lightweight (LAPs) مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يفترض هذا المستند أن نقاط الوصول في الوضع Lightweight (LAP) مسجلة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). ارجع إلى [تسجيل نقطة الوصول في الوضع Lightweight إلى قسم قوائم التحكم في الشبكة المحلية اللاسلكية \(WLCs\) في تجاوز فيش وحدة التحكم في الشبكة المحلية اللاسلكية \(WLAN\) لمثال تكوين نقاط الوصول في الوضع Lightweight](#) للحصول على معلومات حول كيفية تسجيل نقاط الوصول في الوضع Lightweight مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). للمرجع مع مثال التكوين هذا، يتم نشر نقطة الوصول (AP1240S) على شبكة فرعية منفصلة (24/10.10.81.0) من وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) ((10.10.80.0/24))، ويتم إستخدام خيار DHCP رقم 43 لتوفير اكتشاف وحدة التحكم.

## [مصادقة RADIUS من خلال ACS الأمن من Cisco](#)

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

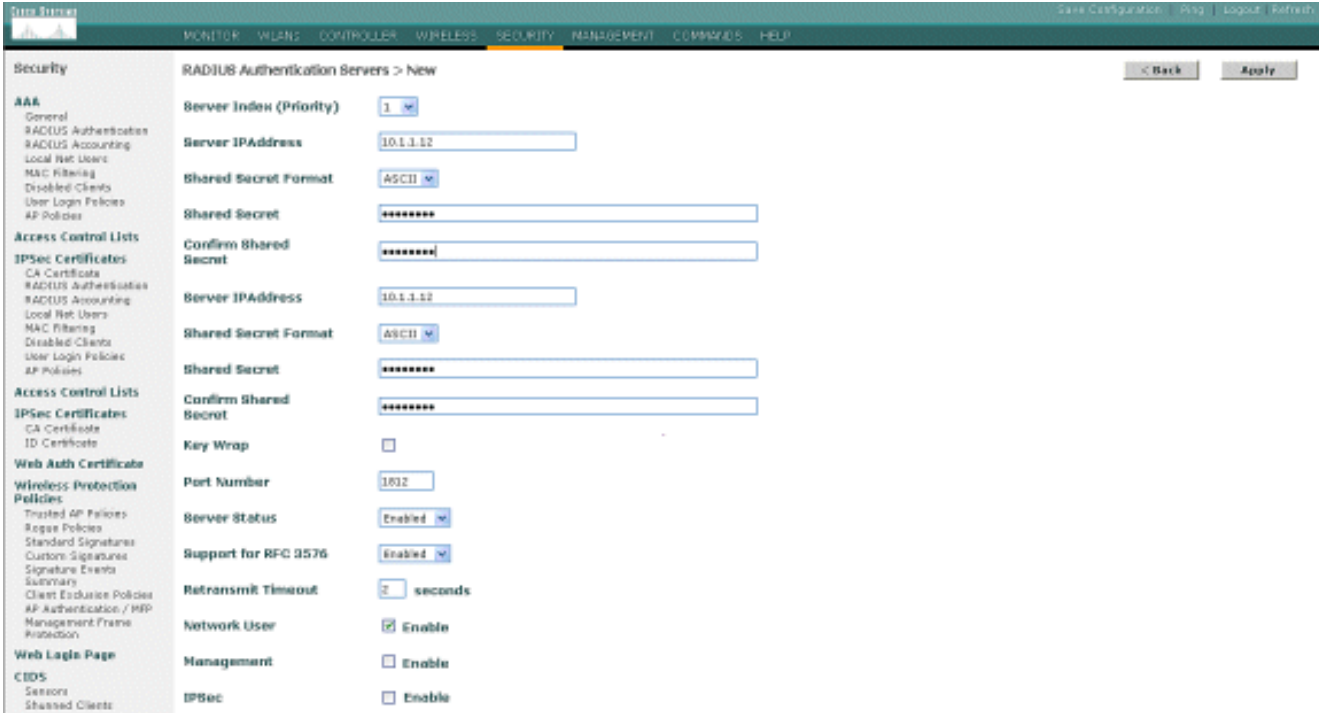
ACS الآمن من Cisco. يتحقق خادم ACS بعد ذلك من مسوغات المستخدم (من خلال قاعدة بيانات Windows التي تم تكوينها) ويوفر الوصول إلى العملاء اللاسلكيين.

أتمت هذا steps أن يشكل ال WLC للاتصال إلى ال ACS نادل:

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



2. قم بتعريف معلومات خادم ACS في خوادم مصادقة RADIUS < صفحة جديدة. وتتضمن هذه المعلومات عنوان IP ل ACS والسر المشترك ورقم المنفذ وحالة الخادم. ملاحظة: رقم المنفذ 1645 أو 1812 متوافق مع ACS لمصادقة RADIUS. تحدد خانة الاختيار لمستخدم الشبكة وإدارتها ما إذا كانت المصادقة المستندة إلى RADIUS تنطبق على مستخدمي الشبكة (على سبيل المثال، عملاء WLAN) والإدارة (أي المستخدمين الإداريين). يستخدم مثال التكوين مصدر المحتوى الإضافي الآمن من Cisco كخادم RADIUS مع عنوان IP 10.1.1.12:



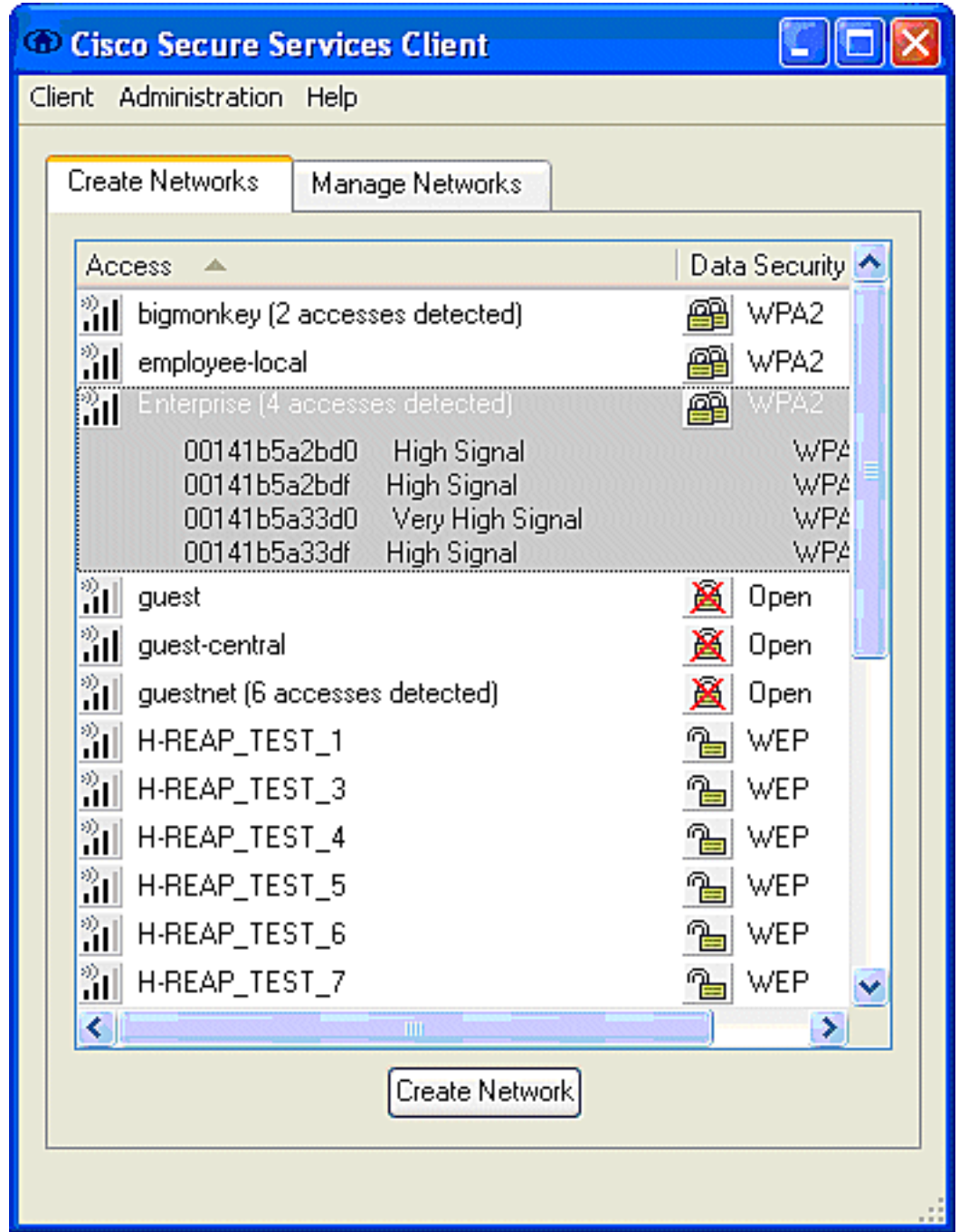
## [تكوين معلومات WLAN](#)

يصف هذا القسم تكوين عميل Cisco Secure Services. في هذا المثال، يتم استخدام CSSC v4.0.5.4783 مع مهائى عميل Cisco CB21AG. قبل تثبيت برنامج CSSC، تحقق من تثبيت برامج تشغيل CB21AG فقط، وليس أداة (Aironet Desktop Utility) (ADU).

بمجرد تثبيت البرنامج وتشغيله كخدمة، فإنه يقوم بفحص الشبكات المتاحة ويعرض الشبكات المتاحة.

ملاحظة: يقوم CSSC بتعطيل تكوين Windows Zero.

ملاحظة: لا يظهر سوى معرف SSID الذي تم تمكينه للبث.



ملاحظة: تقوم وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN)، بشكل افتراضي، ببث SSID، لذلك يظهر في قائمة إنشاء شبكات من SSIDs الممسوحة ضوئياً. لإنشاء توصيف شبكة، يمكنك ببساطة النقر على SSID في القائمة (Enterprise) وزر إنشاء راديو الشبكة.

إذا تم تكوين البنية الأساسية للشبكة المحلية اللاسلكية (WLAN) مع تعطيل Broadcast SSID، يجب إضافة SSID يدوياً، انقر فوق زر إضافة راديو تحت أجهزة الوصول وأدخل يدوياً SSID المناسب (على سبيل المثال، Enterprise). قم بتكوين سلوك المسبار النشط للعميل، أي عندما يقوم العميل بالبحث بنشاط عن معرف SSID المكون الخاص به، حدد البحث النشط عن جهاز الوصول هذا بعد إدخال SSID في نافذة إضافة جهاز الوصول.

ملاحظة: لا تسمح إعدادات المنفذ بأوضاع المؤسسات (802.1X) إذا لم تكن إعدادات مصادقة EAP مكونة لأول مرة للتوصيف.

يطلق زر إنشاء راديو الشبكة إطار ملف تعريف الشبكة، والذي يسمح لك بإقران SSID المختار (أو المكون) بألية مصادقة. قم بتعيين اسم وصفي لملف التعريف.

**ملاحظة:** يمكن إقران أنواع أمان متعددة لشبكة WLAN و/أو SSIDs ضمن ملف تعريف المصادقة هذا.

لكي يتمكن العميل من الاتصال بالشبكة تلقائياً عند وجوده في نطاق تغطية التردد اللاسلكي، أختَر إنشاء اتصال **المستخدم تلقائياً**. إلغاء تحديد **مفتاح لجميع المستخدمين** إذا لم يكن من المرغوب استخدام ملف التعريف هذا مع حسابات المستخدمين الأخرى على الجهاز. إذا لم يتم إختيار **الإنشاء التلقائي**، فمن الضروري للمستخدم فتح نافذة CSSC وبدء اتصال WLAN يدوياً باستخدام زر **توصيل** الراديو.

إذا كان من المطلوب بدء اتصال WLAN قبل دخول المستخدم، أختَر **قبل حساب المستخدم**. وهذا يسمح بعملية تسجيل الدخول الأحادي باستخدام مسوغات المستخدم المحفوظة (كلمة المرور أو الشهادة/البطاقة الذكية عند استخدام TLS ضمن EAP-FAST).

**Network Profile**

**Network**

Name: Enterprise Network

Available to all users (public profile)

Automatically establish Machine connection

Automatically establish User connection

Before user account (supports smartcard/password only)

**Network Configuration Summary:**

Authentication: FAST;

Credentials: Request when needed and remember forever.

Modify...

**Access Devices**

Access / SSID	Mode	Notes
Enterprise	WPA2 Enterprise	

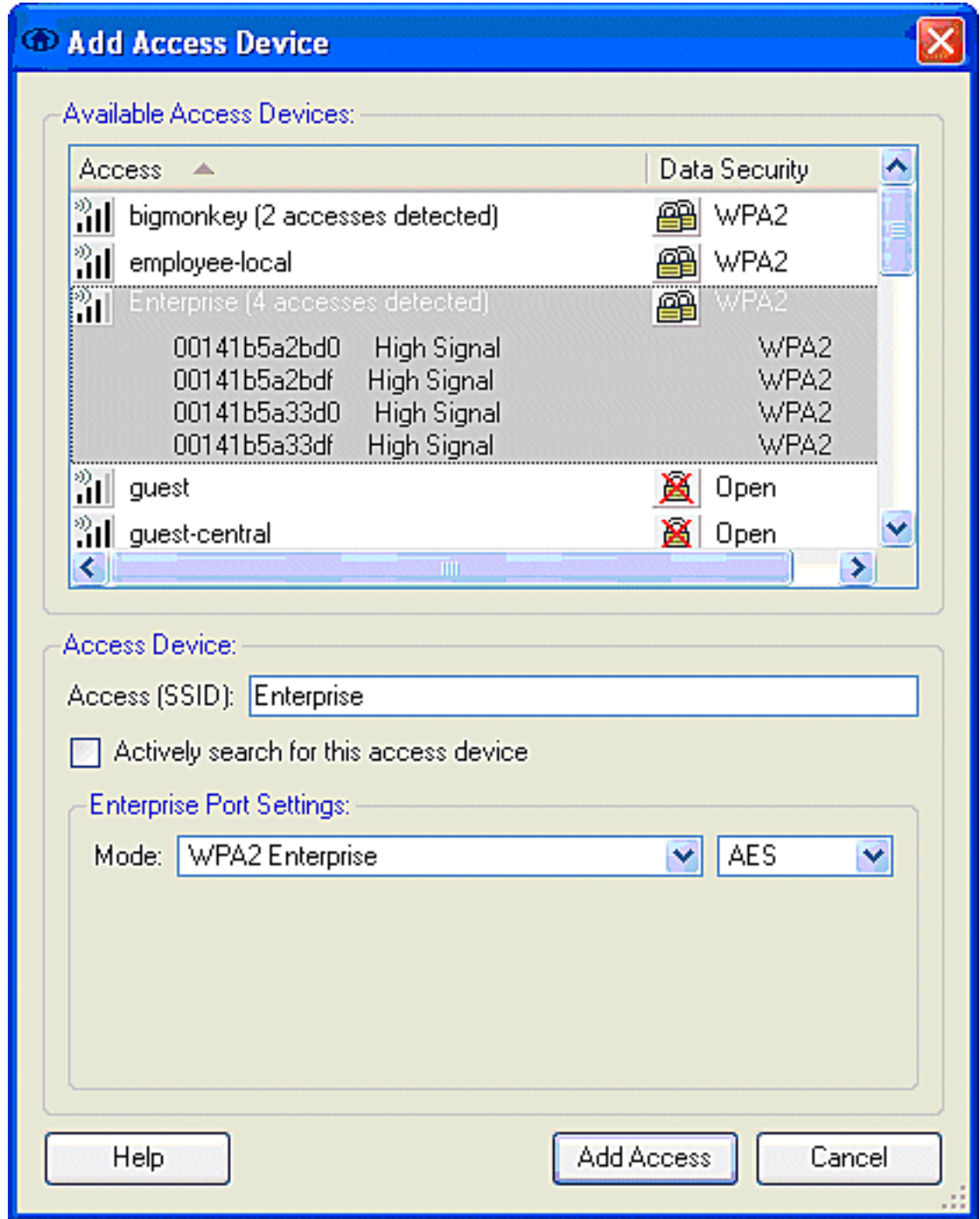
Add... Modify Configuration... Remove

Help OK Cancel

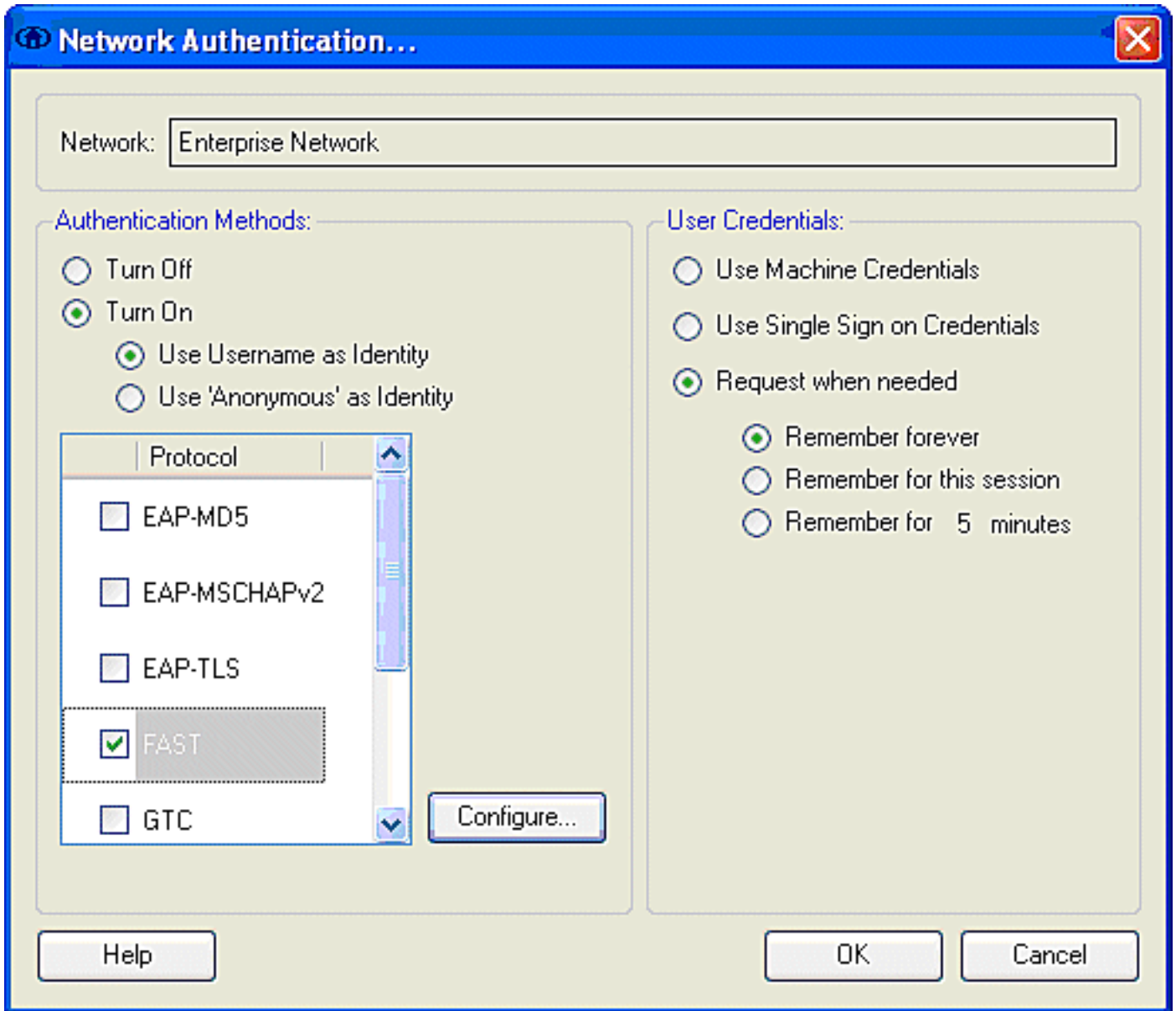
**ملاحظة:** لتشغيل WPA/TKIP مع مهايئ عميل Cisco Aironet 350 Series Client Adapter، من الضروري تعطيل التحقق من صحة مصافحة WPA نظراً لوجود عدم توافق حالياً بين عميل CSSC و 350 محرك فيما يتعلق بالتحقق من صحة تجزئة مصافحة WPA. يتم تعطيل هذا تحت العميل < إعدادات متقدمة > التحقق من صحة تأكيد اتصال



WPA/WPA2. لا يزال التحقق من صحة تأكيد الاتصال المعطل يسمح بميزات الأمان المتأصلة في WPA (TKIP) لكل حزمة كبل وفحص تكامل الرسائل)، ولكنه يعطل مصادقة مفتاح WPA الأولي.



تحت ملخص تكوين الشبكة، انقر على **تعديل** لتكوين إعدادات EAP / بيانات الاعتماد. حدد **تشغيل المصادقة**، واختر **FAST** ضمن البروتوكول، واختر **'مجهول' كهوية** (لاستخدام لا اسم مستخدم في طلب EAP الأولي). من الممكن استخدام اسم المستخدم كمعرف لمعرف EAP الخارجي، ولكن لا يرغب العديد من العملاء في عرض معرفات المستخدم في طلب EAP الأولي غير المشفر. حدد **إستخدام بيانات اعتماد تسجيل الدخول الأحادي** لاستخدام بيانات اعتماد تسجيل الدخول لمصادقة الشبكة. انقر على **تكوين** لإعداد معالم EAP-FAST.



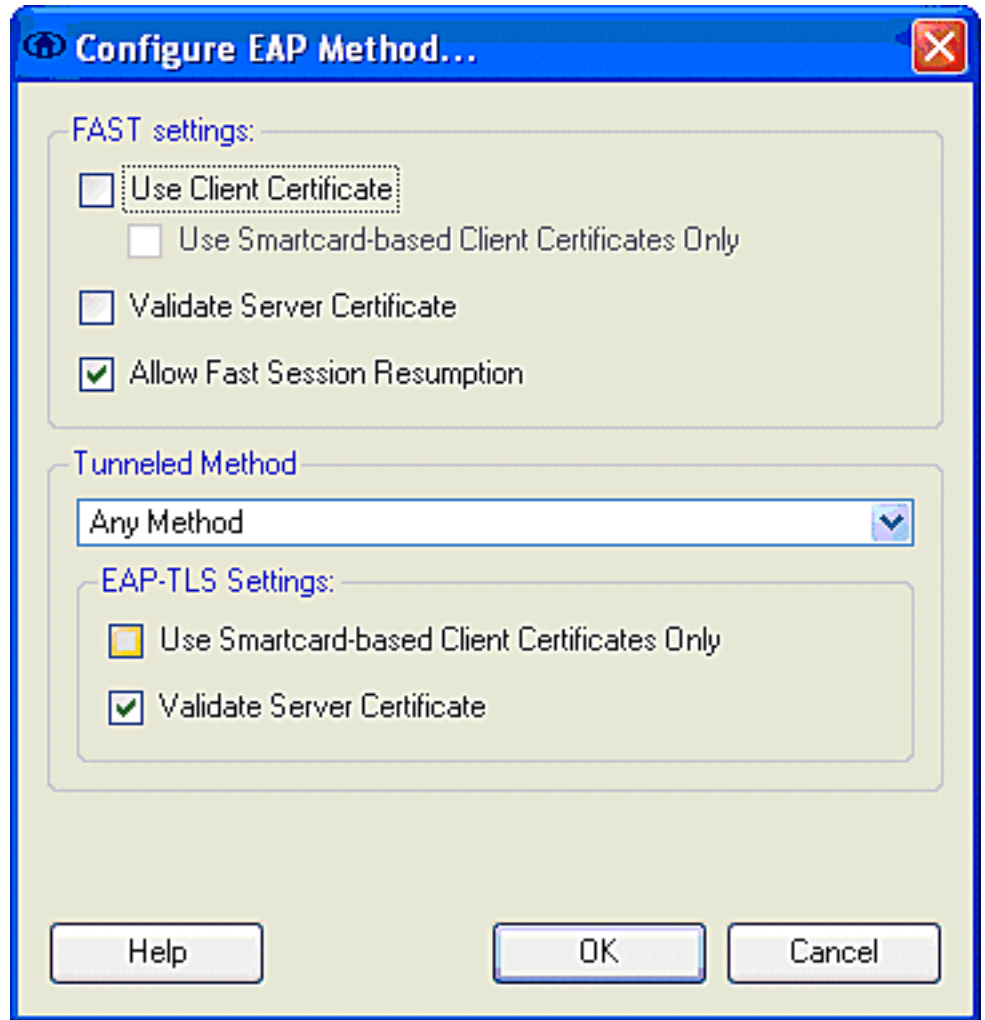
تحت إعدادات FAST، من الممكن تحديد التحقق من شهادة الخادم، والتي تتيح للعميل التحقق من شهادة خادم EAP-FAST (ACS) قبل إنشاء جلسة EAP-FAST. وهذا يوفر الحماية لأجهزة العميل من الاتصال بخادم EAP-FAST مجهول أو دخيل وهمي غير مقصود لبيانات اعتماد المصادقة الخاصة بها إلى مصدر غير موثوق. وهذا يتطلب أن يكون لدى خادم ACS شهادة مثبتة وأن يكون لدى العميل أيضا شهادة المرجع المصدق الجذر الخاص بالمراسل مثبتة. في هذا المثال، لم يتم تمكين التحقق من شهادة الخادم.

تحت إعدادات FAST، من الممكن تحديد السماح باستئناف الجلسة السريعة، والذي يسمح باستئناف جلسة EAP-FAST بناء على معلومات النفق (TLS) بدلا من متطلبات إعادة مصادقة EAP-FAST كاملة. إذا كان لدى خادم EAP-FAST والعميل معرفة مشتركة بمعلومات جلسة TLS التي تم التفاوض عليها ضمن تبادل مصادقة EAP-FAST الأولى، يمكن أن يحدث استئناف الجلسة.

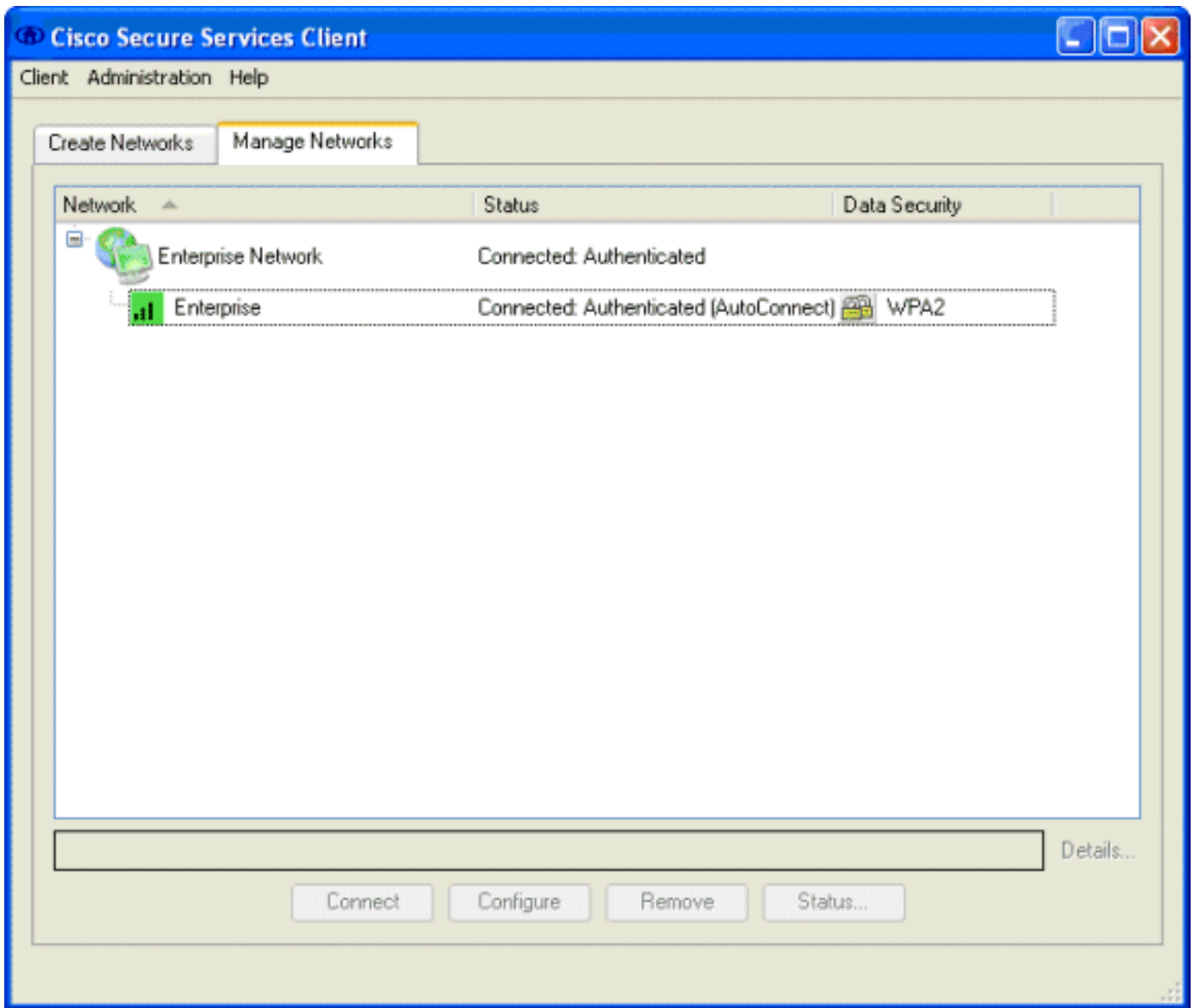
**ملاحظة:** يجب تكوين كل من خادم EAP-FAST والعميل لاستئناف جلسة EAP-FAST.

تحت أسلوب النطاقات < إعدادات EAP-TLS، حدد أي طريقة للسماح بالتزويد التلقائي ل EAP-MSCHAPv2 ل PAC و EAP-GTC للمصادقة. إذا كنت تستخدم قاعدة بيانات بتنسيق Microsoft، مثل Active Directory، وإذا لم تكن تدعم أي عملاء EAP-FAST v1 على الشبكة، فيمكنك أيضا تحديد استخدام MSCHAPv2 فقط كطريقة ذات قنوات.

**ملاحظة:** يتم تمكين التحقق من شهادة الخادم بشكل افتراضي ضمن إعدادات EAP-TLS في هذا الإطار. بما أن المثال لا يستخدم EAP-TLS كطريقة مصادقة داخلية، فإن هذا الحقل غير قابل للتطبيق. في حالة تمكين هذا الحقل، فإنه يمكن العميل من التحقق من شهادة الخادم بالإضافة إلى التحقق من صحة شهادة العميل داخل EAP-TLS.



انقر على **موافق** لحفظ إعدادات EAP-FAST. بما أن العميل تم تكوينه لـ "الإنشاء التلقائي" تحت التوصيف، فإنه يقوم تلقائياً ببدء الاقتران/المصادقة مع الشبكة. من علامة التبويب إدارة الشبكات، تشير حقول الشبكة والحالة وأمان البيانات إلى حالة اتصال العميل. ومن هذا المثال، يتبين أن توصيف المؤسسة قيد الاستخدام وأداة الوصول إلى الشبكة هي مؤسسة SSID، والتي تشير إلى متصل:مصدق ويستخدم التوصيل التلقائي. يشير الحقل "أمان البيانات" إلى نوع تشفير 802.11 المستخدم، والذي، على سبيل المثال، هو WPA2.



بعد مصادقة العميل، أختار SSID ضمن ملف التعريف في علامة التبويب إدارة الشبكات وانقر فوق الحالة للاستعلام عن تفاصيل الاتصال. يوفر إطار تفاصيل الاتصال معلومات عن جهاز العميل وحالة الاتصال وإحصاءاته وطريقة المصادقة. توفر علامة تبويب تفاصيل WiFi تفاصيل عن حالة توصيل 11.802 الذي يتضمن RSSI والقناة 11.802 والمصادقة/التشفير.

## Connection Status



Connection Details

WiFi Details

Status: Connected: Authenticated

Duration: 00:00:47

Network Profile: Enterprise Network

Network Adapter: Cisco Aironet 802.11 a/b/g Wireless Adapter (Microsoft's Packet Scheduler)

Client MAC Address: 00-40-96-A0-36-2F

Access Device: Enterprise

Access Device MAC Address: 00-14-1B-5A-33-D0

Transmitted packets: 121

Received packets: 6

Speed: 54.0 Mbps

Authentication Method: FAST / GTC

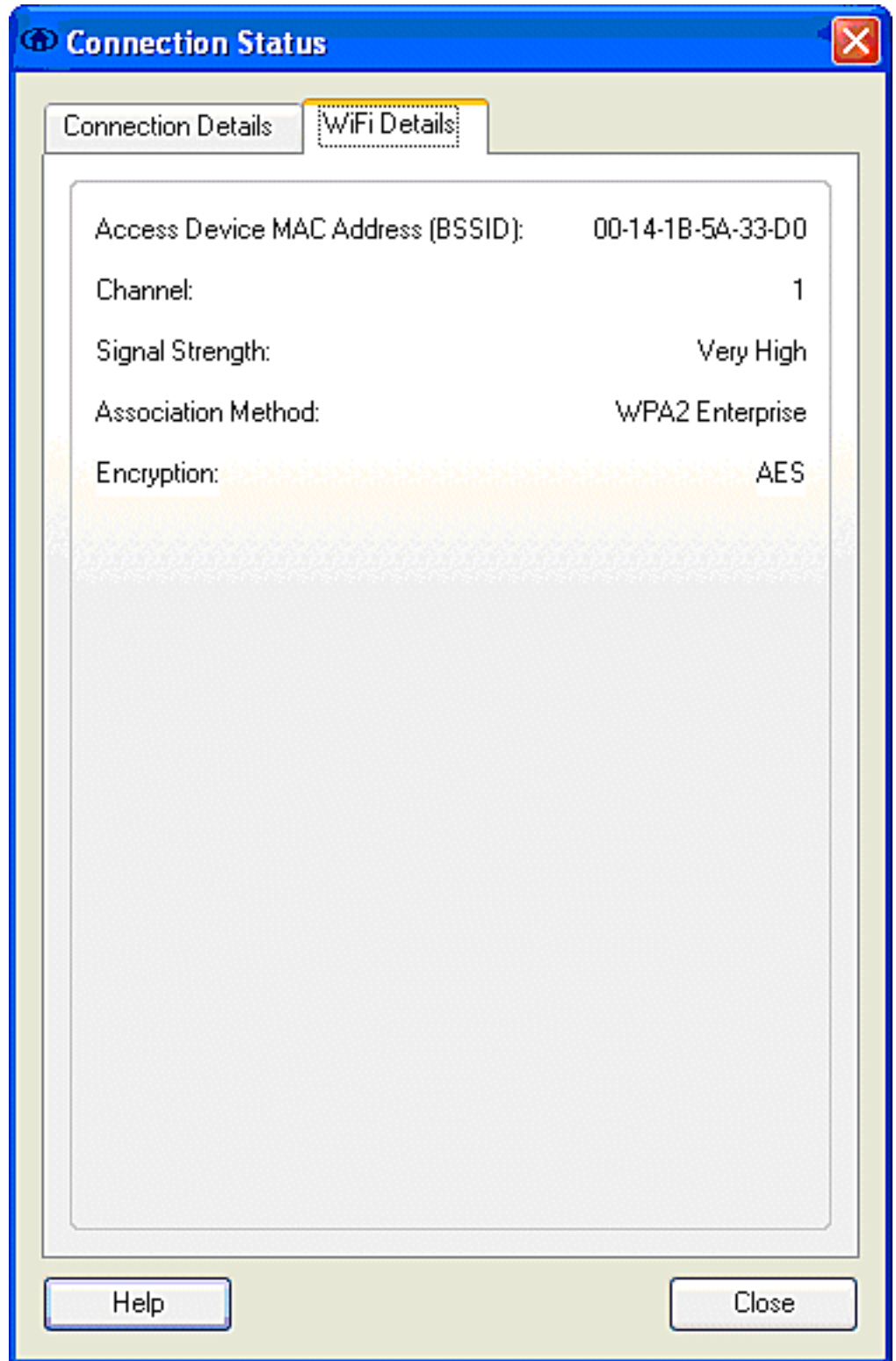
Authentication Server: TME (not verified)

IP Address: 10.10.82.11

Help

Close





بصفتك مسؤول نظام، يحق لك الحصول على الأداة المساعدة التشخيصية، وتقرير نظام Cisco Secure Services Client، المتوفر مع توزيع CSSC القياسي. تتوفر هذه الأداة المساعدة من القائمة "أبدأ" أو من دليل CSSC. للحصول على البيانات، انقر فوق **تجميع البيانات > نسخ إلى الحافظة > تحديد موقع ملف التقرير**. يقوم هذا بتوجيه نافذة Microsoft File Explorer إلى الدليل باستخدام ملف التقرير المضغوط. ضمن الملف المضغوط، تقع أكثر البيانات فائدة تحت السجل (log\_current).

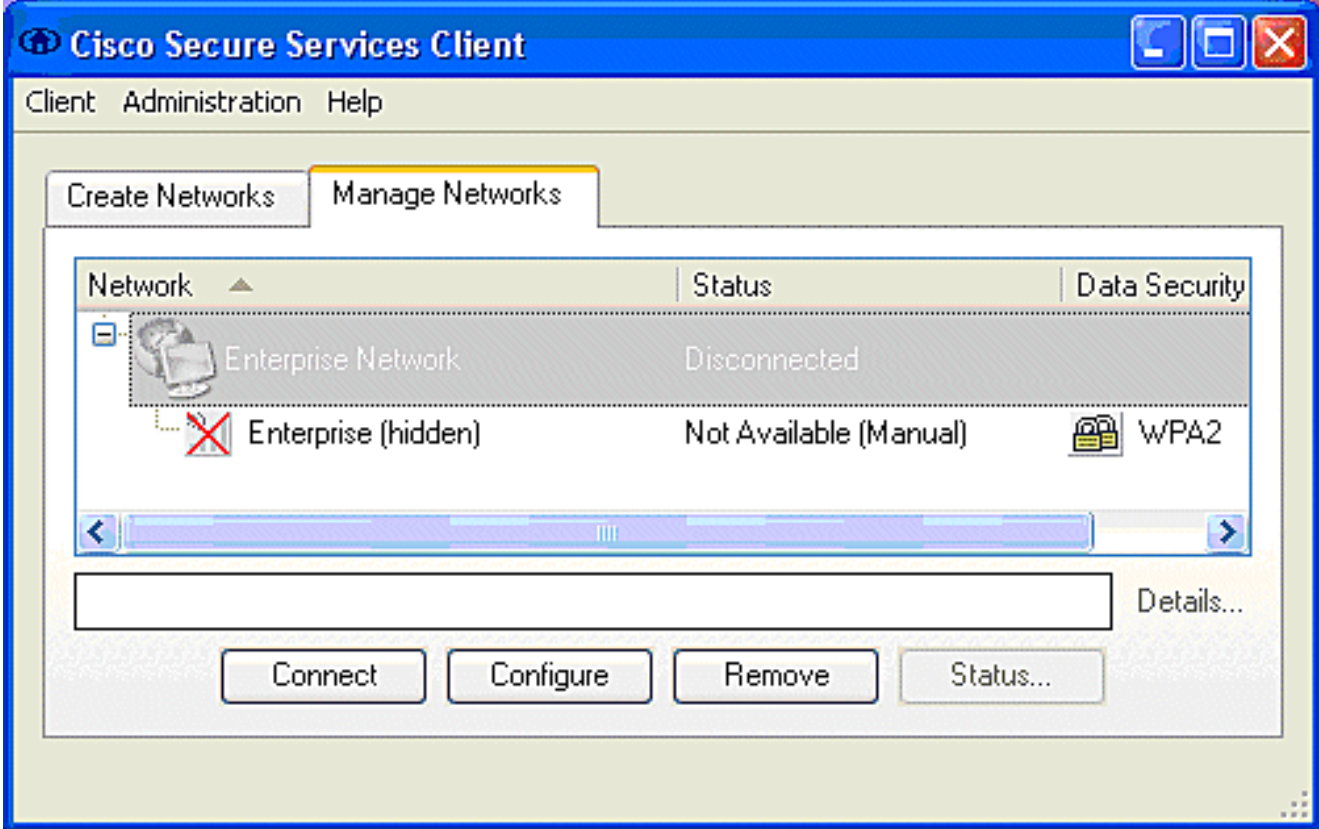
تقدم الأداة المساعدة الحالة الحالية لتفاصيل CSSC والواجهة وبرنامج التشغيل بالإضافة إلى معلومات الشبكة المحلية اللاسلكية (WLAN Information (SSID Detected) وحالة الاقتران، وما إلى ذلك). يمكن أن يكون هذا مفيداً، خاصة لتشخيص مشاكل الاتصال بين CSSC ومهايم الشبكة المحلية اللاسلكية (WLAN).

[التحقق من العملية](#)

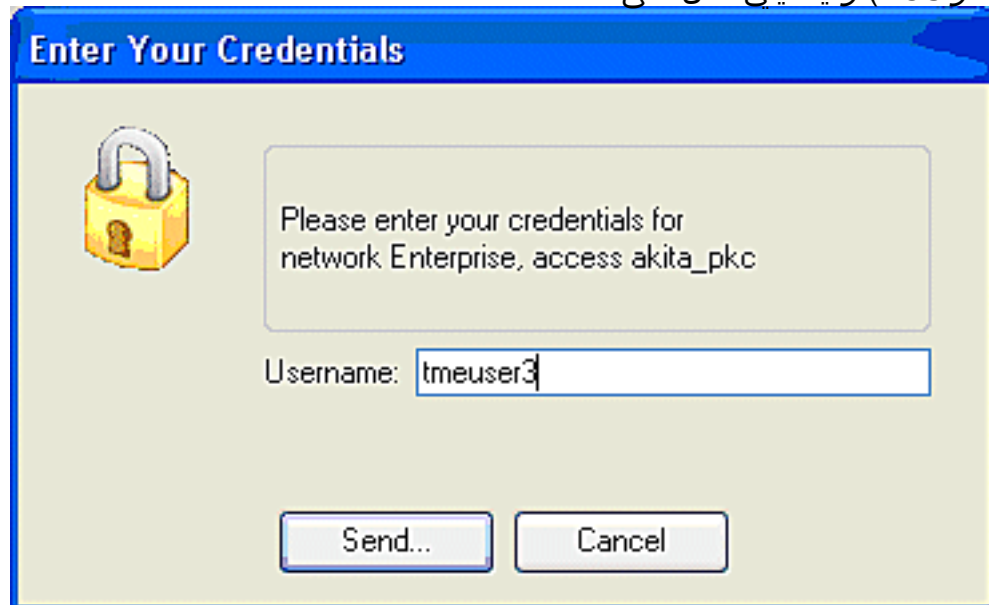
بعد تكوين خادم Cisco Secure ACS، ووحدة تحكم الشبكة المحلية اللاسلكية (WLAN)، وعمليات CSSC، ونسخ تكوين قاعدة البيانات وتصحيحها المفترض، يتم تكوين شبكة WLAN لمصادقة EAP-FAST واتصال العميل الآمن. هناك نقاط عديدة يمكن مراقبتها للتحقق من التقدم / الأخطاء لجلسة عمل آمنة.

لاختبار التكوين، حاول إقران عميل لاسلكي بوحدة التحكم في الشبكة المحلية اللاسلكية بمصادقة EAP-FAST.

1. إذا تم تكوين CSSC للاتصال التلقائي، يحاول العميل هذا الاتصال تلقائياً. إذا لم يتم تكوينه للاتصال التلقائي وعمليات تسجيل الدخول الأحادي، فيجب على المستخدم بدء اتصال WLAN من خلال زر **توصيل** الراديو. وهذا يؤدي إلى بدء عملية اقتران 802.11 التي تحدث من خلالها مصادقة EAP. وفيما يلي مثال على هذا:




2. ثم يطلب من المستخدم توفير اسم المستخدم ثم كلمة المرور لمصادقة EAP-FAST (من مرجع EAP-FAST PAC أو ACS). وفيما يلي مثال على هذا:



هذا:

## Enter Your Credentials



Please enter your credentials for network Enterprise, access akita\_pkc

Username:

Welcome to the Richfield TME PAC Auth

Dialog expires in 10 second(s)...

3. يقوم عميل CSSC، عن طريق عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، بعد ذلك بتمرير بيانات اعتماد المستخدم إلى خادم (RADIUS) (Cisco Secure ACS) للتحقق من بيانات الاعتماد. يتحقق ACS من مسوغات المستخدم عن طريق عقد مقارنة بين البيانات وقاعدة البيانات التي تم تكوينها (في مثال التكوين، تكون قاعدة البيانات الخارجية هي Windows Active Directory) ويوفر الوصول إلى العميل اللاسلكي كلما كانت مسوغات المستخدم صالحة. يظهر تقرير المصادقة الذي تم تمريره على خادم ACS أن العميل قد اجتاز مصادقة RADIUS/EAP. وفيما يلي مثال على هذا:

**Reports and Activity**

Select

Passed Authentications active.csv

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

Filtering is not applied.

Date	Time	Message- Type	User- Name	Group- Name	Caller- ID	NAS- Port	NAS-IP- Address	Network Access Profile Name	Shared BAG	Downloadable ACL	System- Posture- Token	Application- Posture- Token	Reason	EA Type
08/22/2006	16:25:37	Authen OK	test	Default Group	00-40-96-A0-36-2F	29	10.10.80.3	(Default)	..	..	..	..	..	43
08/22/2006	16:09:51	Authen OK	test	Default Group	00-40-96-A6-D5-F6	29	10.10.80.3	(Default)	..	..	..	..	..	43
08/22/2006	16:06:55	Authen OK	test	Default Group	00-40-96-A6-D5-F6	29	10.10.80.3	(Default)	..	..	..	..	..	43
08/22/2006	16:06:39	Authen OK	test	Default Group	00-40-96-A6-D5-F6	29	10.10.80.3	(Default)	..	..	..	..	..	43
08/22/2006	16:06:29	Authen OK	test	Default Group	00-40-96-A6-D5-F6	29	10.10.80.3	(Default)	..	..	..	..	..	43

4. على مصادقة RADIUS/EAP الناجحة، تتم مصادقة العميل اللاسلكي (ab:36:2f:00:40:96 في هذا المثال) مع وحدة التحكم في نقطة الوصول/الشبكة المحلية اللاسلكية (WLAN).

**Wireless**

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Wireless Clients

Search by MAC address

Client MAC Addr	AP Name	WLAN	Type	Status	Auth	Port
88:0f:b5:45:04:30	AP0004.6948.9504	Unknown	882.11b	Probing	No	29
88:0f:96:a0:36:2f	AP0004.6948.9504	Enterprise	882.11g	Associated	Yes	29
88:0f:96:a0:d0:69	AP0004.6948.9480	Unknown	882.11b	Probing	No	29
88:0f:96:a0:d0:19	AP0004.6948.9480	Enterprise	882.11g	Associated	No	29

بالإضافة إلى معلومات التشخيص والحالة، المتاحة في وحدة التحكم في ACS الآمنة من Cisco و Cisco WLAN، هناك نقاط إضافية يمكن استخدامها لتشخيص مصادقة EAP-FAST. على الرغم من أنه يمكن تشخيص معظم مشاكل المصادقة دون استخدام sniffer للشبكة المحلية اللاسلكية (WLAN) أو تصحيح أخطاء عمليات تبادل EAP في وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN)، إلا أنه يتم تضمين هذه المواد المرجعية للمساعدة في استكشاف الأخطاء وإصلاحها.

## EAP-FAST Exchange ل sniffer التقاط

ييدي هذا 802.11 sniffer التقاط المصادقة تبادل.

Source	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
00:14:1B:5A:33:D0	*	11	68%	36.0	101	00.033877	802.11 Assoc Req	FC=...R.....,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0	*	11	70%	24.0	101	00.036453	802.11 Assoc Req	FC=...R.....,SN=2867,FM= 0,Status...
00:14:1B:5A:33:D0		11	71%	54.0	90	00.036494	802.Ix	FC=.F.....,SN=2868,FM= 0
Aironet:A0:36:2F		11	54%	1.0	82	00.123205	EAP Response	FC=T.....,SN= 3,FM= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.123517	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	65	00.165611	802.Ix	FC=.F.....,SN=2870,FM= 0
Aironet:A0:36:2F		11	55%	1.0	82	00.173920	EAP Response	FC=T.....,SN= 4,FM= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.174228	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	66	00.178863	802.Ix	FC=.F.....,SN=2871,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.200632	EAP Response	FC=T.....,SN= 5,FM= 0
Aironet:A0:36:2F		11	58%	1.0	282	00.203340	EAP Response	FC=T.....,SN= 5,FM= 0
00:14:1B:5A:33:D0	#	11	71%	1.0	14	00.203639	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	70%	54.0	188	00.207634	802.Ix	FC=.F.....,SN=2872,FM= 0
Aironet:A0:36:2F		11	55%	1.0	105	00.216295	EAP Response	FC=T.....,SN= 6,FM= 0
Aironet:A0:36:2F		11	57%	1.0	105	00.217444	EAP Response	FC=T..R.....,SN= 6,FM= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.217754	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	67%	54.0	99	00.222799	802.Ix	FC=.F.....,SN=2874,FM= 0
Aironet:A0:36:2F		11	55%	1.0	152	00.254189	EAP Response	FC=T.....,SN= 7,FM= 0
00:14:1B:5A:33:D0	#	11	68%	1.0	14	00.254499	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	64%	54.0	147	00.288950	802.Ix	FC=.F.R.....,SN=2875,FM= 0
Aironet:A0:36:2F		11	55%	1.0	232	00.318087	EAP Response	FC=T.....,SN= 8,FM= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.318383	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	68%	54.0	44	00.326833	802.Ix	FC=.F.....,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	65%	54.0	44	00.326882	802.Ix	FC=.F.R.....,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	48.0	44	00.326922	802.Ix	FC=.F.R.....,SN=2877,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	157	00.326964	802.Ix	FC=.F.....,SN=2878,FM= 0
Aironet:A0:36:2F		11	57%	1.0	157	00.333742	EAP01-Key	FC=T.....,SN= 9,FM= 0
00:14:1B:5A:33:D0	#	11	70%	1.0	14	00.334019	802.11 Ack	FC=.....
00:14:1B:5A:33:D0		11	65%	54.0	207	00.340467	802.Ix	FC=.F.....,SN=2879,FM= 0
00:14:1B:5A:33:D0		11	67%	54.0	207	00.341130	802.Ix	FC=.F.R.....,SN=2879,FM= 0
Aironet:A0:36:2F		11	57%	1.0	135	00.342542	EAP01-Key	FC=T.....,SN= 10,FM= 0

تظهر هذه الحزمة إستجابة EAP-FAST الأولية.

ملاحظة: حسب تكوين عميل CSSC، يستخدم مجهول الهوية كهوية EAP الخارجية في إستجابة EAP الأولية.



## تصحيح الأخطاء في وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN)

يمكن استخدام أوامر تصحيح الأخطاء هذه في وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) لمراقبة تقدم تبادل المصادقة:

- debug aaa events enable
- enable debug aaa detail
- debug dot1x يمكن
- enable debug dot1x الحالات

هذا مثال على بدء حركة مصادقة بين عميل CSSC و ACS كما هو مراقب في وحدة التحكم في الشبكة المحلية اللاسلكية (WLAN) مع تصحيح الأخطاء:

```
,Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing RSN IE type 48
length 20 for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received RSN IE with
PMKIDs from mobile 00:40:96:a0:36:2f 0
- Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x
moving mobile 00:40:96:a0:36:2f into Connecting state
-Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP
(Request/Identity to mobile 00:40:96:a0:36:2f (EAP Id 1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Identity Response
count=1) from mobile 00:40:96:a0:36:2f)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f EAP State update from
Connecting to Authenticating for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x - moving mobile
a0:36:2f into Authenticating state:00:40:96
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth
Response state for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AuthenticationRequest: 0x138dd764
Thu Aug 24 18:20:54 2006: Callback.....0x10372764
Thu Aug 24 18:20:54 2006: protocolType...0x00040001
Thu Aug 24 18:20:54 2006: proxyState....00:40:96:A0:36:2F-11:00
(Thu Aug 24 18:20:54 2006: Packet contains 15 AVPs (not shown
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Successful transmission of
```



```

Authentication Packet (id 84) to 10.1.1.12:1812, proxy state0
Thu Aug 24 18:20:54 2006: ****Enter processIncomingMessages: response code=11
Thu Aug 24 18:20:54 2006: ****Enter processRadiusResponse: response code=11
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Access-Challenge received from
RADIUS server 10.1.1.12 for mobile 00:40:96:a0:36:2f rec7
Thu Aug 24 18:20:54 2006: AuthorizationResponse: 0x11c8a394
Thu Aug 24 18:20:54 2006:      structureSize..147
Thu Aug 24 18:20:54 2006:      resultCode.....255
Thu Aug 24 18:20:54 2006:      protocolUsed...0x00000001
Thu Aug 24 18:20:54 2006:      proxyState.....00:40:96:A0:36:2F-11:00
(Thu Aug 24 18:20:54 2006:      Packet contains 4 AVPs (not shown
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access-Challenge
for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend Auth Req state
id=249) for mobile 00:40:96:a0:36:2f)
:Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f WARNING
updated EAP-Identifer 1 ==> 249 for STA 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP Request from
(AAA to mobile 00:40:96:a0:36:2f (EAP Id 249
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAP Response from
(mobile 00:40:96:a0:36:2f (EAP Id 249, EAP Type 3

```

هذا هو الإكمال الناجح لتبادل EAP من تصحيح أخطاء وحدة التحكم (مع مصادقة WPA2):

```

-Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Processing Access
Accept for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Applying new AAA
override for station 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Override values for station
a0:36:2f source: 4, valid bits: 0x0:00:40:96
:qosLevel: -1, dscp: 0xffffffff, dot1pTag: 0xffffffff, sessionTimeout
'dataAvgC: -1, rTAVGC: -1, dataBurstC: -1, rl -1
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Unable to apply override
policy for station 00:40:96:a0:36:2f - VapAllowRadiusOverride E
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Creating a new PMK Cache Entry
(for station 00:40:96:a0:36:2f (RSN 2
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Adding BSSID
00:14:1b:5a:33:d0 to PMKID cache for station 00:40:96:a0:36:2f
(Thu Aug 24 18:20:54 2006: New PMKID: (16
Thu Aug 24 18:20:54 2006:      [0000] a6 c0 02 95 66 e8 ed 9b 1c 65 9b
1f 3f 5f 5b 72
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAP-Success
(to mobile 00:40:96:a0:36:2f (EAP Id 0
(Thu Aug 24 18:20:54 2006: Including PMKID in M1 (16
:Thu Aug 24 18:20:54 2006
a6 c0 02 95 66 e8 ed 9b 1c 65 9b 72 1f 3f 5f 5b [0000]
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message to
mobile 00:40:96:a0:36:2f state INITPMK (message 1), repl0
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Entering Backend
Auth Success state (id=0) for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received Auth Success
while in Authenticating state for mobile 00:40:96:a0:36:2f
- Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f dot1x
moving mobile 00:40:96:a0:36:2f into Authenticated state
-Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL
Key from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version
in EAPOL-key message from mobile 00:40:96:a0:36:2f (1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key
in PKT_START state (message 2) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Stopping retransmission

```

```

timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Sending EAPOL-Key Message
to mobile 00:40:96:a0:36:2f state PTKINITNEGOTIATING (message 1)
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received
EAPOL-Key from mobile 00:40:96:a0:36:2f
(Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Invalid EAPOL version (1
in EAPOL-key message from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f Received EAPOL-key in
PTKINITNEGOTIATING state (message 4) from mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:54 2006: AccountingMessage
Accounting Interim: 0x138dd764
:Thu Aug 24 18:20:54 2006: Packet contains 20 AVPs
:Thu Aug 24 18:20:54 2006
(AVP[01] User-Name.....enterprise (10 bytes
[Thu Aug 24 18:20:54 2006: AVP[02
(Nas-Port.....0x0000001d (29) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[03
(Nas-IP-Address.....0x0a0a5003 (168448003) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[04
(Class.....CACs:0/28b5/a0a5003/29 (22 bytes
[Thu Aug 24 18:20:54 2006: AVP[05
(NAS-Identifier.....ws-3750 (7 bytes
[Thu Aug 24 18:20:54 2006: AVP[06
(Airespace / WLAN-Identifier.....0x00000001 (1) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[07
:Acct-Session-Id.....44ede3b0/00:40
(a0:36:2f/14 (29 bytes:96
[Thu Aug 24 18:20:54 2006: AVP[08
(Acct-Authentic.....0x00000001 (1) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[09
(Tunnel-Type.....0x0000000d (13) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[10
(Tunnel-Medium-Type.....0x00000006 (6) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[11
(Tunnel-Group-Id.....0x3832 (14386) (2 bytes
[Thu Aug 24 18:20:54 2006: AVP[12
(Acct-Status-Type.....0x00000003 (3) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[13
(Acct-Input-Octets.....0x000b99a6 (760230) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[14
(Acct-Output-Octets.....0x00043a27 (277031) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[15
(Acct-Input-Packets.....0x0000444b (17483) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[16
(Acct-Output-Packets.....0x0000099b (2459) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[17
(Acct-Session-Time.....0x00000a57 (2647) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[18
(Acct-Delay-Time.....0x00000000 (0) (4 bytes
[Thu Aug 24 18:20:54 2006: AVP[19
(Calling-Station-Id.....10.10.82.11 (11 bytes
[Thu Aug 24 18:20:54 2006: AVP[20
(Called-Station-Id.....10.10.80.3 (10 bytes
Thu Aug 24 18:20:54 2006: 00:40:96:a0:36:2f
Stopping retransmission timer for mobile 00:40:96:a0:36:2f
Thu Aug 24 18:20:57 2006: User admin authenticated

```

## معلومات ذات صلة

- [دليل تثبيت Cisco Secure ACS لخادم Windows](#)
- [دليل التكوين ل Cisco Secure ACS 4.1](#)
- [تقييد الوصول إلى شبكة WLAN استنادا إلى SSID باستخدام WLC ومثال تكوين ACS الآمن من Cisco](#)

- EAP-TLS تحت شبكة لاسلكية موحدة مع ACS 4.0 و Windows 2003
- تعيين شبكة VLAN الديناميكية مع مثال تكوين خادم RADIUS ووحدة تحكم شبكة LAN اللاسلكية
- الدعم التقني والمستندات - Cisco Systems

