RSA SecureID جاهز مع وحدات التحكم في الشبكة المحلية اللاسلكية ومثال تكوين Cisco Secure ACS

المحتويات

المقدمة

يشرح هذا المستند كيفية إعداد وتكوين نقاط الوصول من Cisco التي تعمل ببروتوكول نقطة الوصول في الوضع Lightweight (LWAPP) ووحدات التحكم في الشبكة المحلية (LAN) اللاسلكية (WLCs)، وكذلك خادم التحكم في الوصول الآمن (ACS) من Cisco الذي سيتم إستخدامه في بيئة شبكة محلية لاسلكية (WLAN) مصدق عليها بواسطة RSA SecureID. يمكن العثور على أدلة التنفيذ الخاصة ب RSA SecurID على www.rsasecured.com.

المتطلبات الأساسية

المتطلبات

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

- معرفة التحكم في الشبكة المحلية اللاسلكية (WLCs) وكيفية تكوين معلمات WLC الأساسية.
- معرفة كيفية تكوين ملف تعريف Cisco Wireless Client باستخدام ADU (Aironet Desktop Utility).
- معرفة وظائف Cisco Secure ACS.
- معرفة أساسية ب LWAPP.

- لديهم فهم أساسي لخدمات Microsoft Windows Active Directory (AD)، بالإضافة إلى مفاهيم وحدة التحكم بالمجال و DNS.**ملاحظة:** قبل أن تحاول إجراء هذا التكوين، تأكد من أن ACS وخادم إدارة مصادقة RSA موجودين في نفس المجال وأن ساعة النظام الخاصة بهما متزامنة تماما. إذا كنت تستخدم Microsoft Windows AD Services، فارجع إلى وثائق Microsoft لتكوين خادم ACS و RSA Manager في نفس المجال. ارجع إلى تكوين Active Directory وقاعدة بيانات مستخدم Windows للحصول على المعلومات ذات الصلة.

المكونات المستخدمة

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

- مدير مصادقة RSA 6.1
- وكيل مصادقة RSA 6.1 لنظام التشغيل Microsoft Windows
- Cisco Secure ACS 4.0(1) Build 27**ملاحظة:** يمكن إستخدام خادم RADIUS المضمن بدلا من مصدر المحتوى الإضافي من Cisco. راجع وثائق RADIUS التي تم تضمينها مع مدير مصادقة RSA حول كيفية تكوين الخادم.
- نقاط الوصول من Cisco WLCs وخفيف الوزن الإصدار 4.0 (الإصدار 4.0.155.0)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة 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

نظام RSA SecureID هو حل مصادقة مستخدم ثنائي العوامل. عند إستخدامه بالاقتران مع مدير مصادقة RSA ووكيل مصادقة RSA، يتطلب مصدق RSA SecureID من المستخدمين تعريف أنفسهم باستخدام آلية مصادقة ثنائية العوامل.

أحدهما هو رمز RSA SecureID، وهو رقم عشوائي يتم إنشاؤه كل 60 ثانية على جهاز مصدق RSA SecureID. والآخر هو رقم التعريف الشخصي (PIN).

تتميز مصادقة RSA SecurID بالسهولة نفسها التي يتم إستخدامها عند إدخال كلمة المرور. يتم تعيين مصدق RSA SecureID لكل مستخدم نهائي يقوم بإنشاء رمز إستخدام مرة واحدة. عند تسجيل الدخول، يقوم المستخدم بإدخال هذا الرقم ببساطة وإدخال رمز PIN سري للمصادقة عليه بنجاح. وكميزة إضافية، عادة ما تكون رموز أجهزة RSA SecureID المميزة مبرمجة بشكل مسبق لتعمل بشكل كامل عند الاستلام.

يشرح عرض الفلاش هذا كيفية إستخدام جهاز مصدق RSA SecureID: عرض RSA.

من خلال برنامج RSA SecureID Ready، تدعم خوادم Cisco WLCs و Cisco Secure ACS مصادقة RSA SecureID بمجرد إخراج الجهاز من عبوته. يعترض برنامج وكيل مصادقة RSA طلبات الوصول، سواء كانت محلية أو عن بعد، من المستخدمين (أو مجموعات المستخدمين) ويوجههم إلى برنامج مدير مصادقة RSA للمصادقة.

يعد برنامج مدير مصادقة RSA هو مكون الإدارة لحل RSA SecureID. ويتم إستخدامه للتحقق من طلبات المصادقة والإدارة المركزية لسياسات المصادقة لشبكات المؤسسات. يعمل بالاقتران مع أجهزة مصادقة RSA SecureID وبرنامج وكيل مصادقة RSA.

في هذا المستند، يتم إستخدام خادم Cisco ACS كعميل مصادقة RSA من خلال تثبيت البرنامج الوكيل عليه. WLC هو خادم الوصول إلى الشبكة (NAS) (عميل AAA) الذي يقوم بدوره بإعادة توجيه مصادقة العميل إلى ACS. يوضح المستند المفاهيم والإعداد باستخدام مصادقة عميل بروتوكول المصادقة المتوسع المحمي (PEAP).

لمعرفة المزيد عن مصادقة PEAP، ارجع إلى بروتوكول المصادقة المتوسع المحمي من Cisco.

التكوين

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

يستخدم هذا المستند التكوينات التالية:

- تكوين مضيف الوكيل
- تكوين وكيل المصادقة

تكوين مضيف الوكيل

إستخدام Cisco Secure ACS كخادم RADIUS

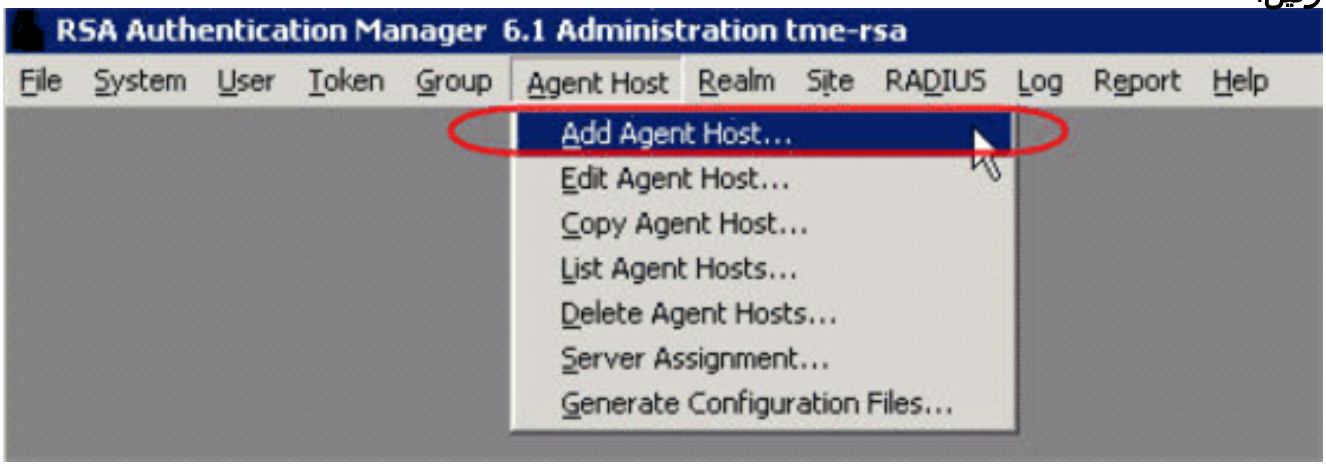
من أجل تسهيل الاتصال بين Cisco Secure ACS وتطبيق RSA Authentication Manager / RSA SecureID Appliance، يجب إضافة سجل مضيف وكيل إلى قاعدة بيانات مدير مصادقة RSA. يحدد سجل مضيف الوكيل ACS الآمن من Cisco ضمن قاعدة بياناته ويحتوي على معلومات حول الاتصال والتشفير.

لإنشاء سجل مضيف الوكيل، تحتاج إلى هذه المعلومات:

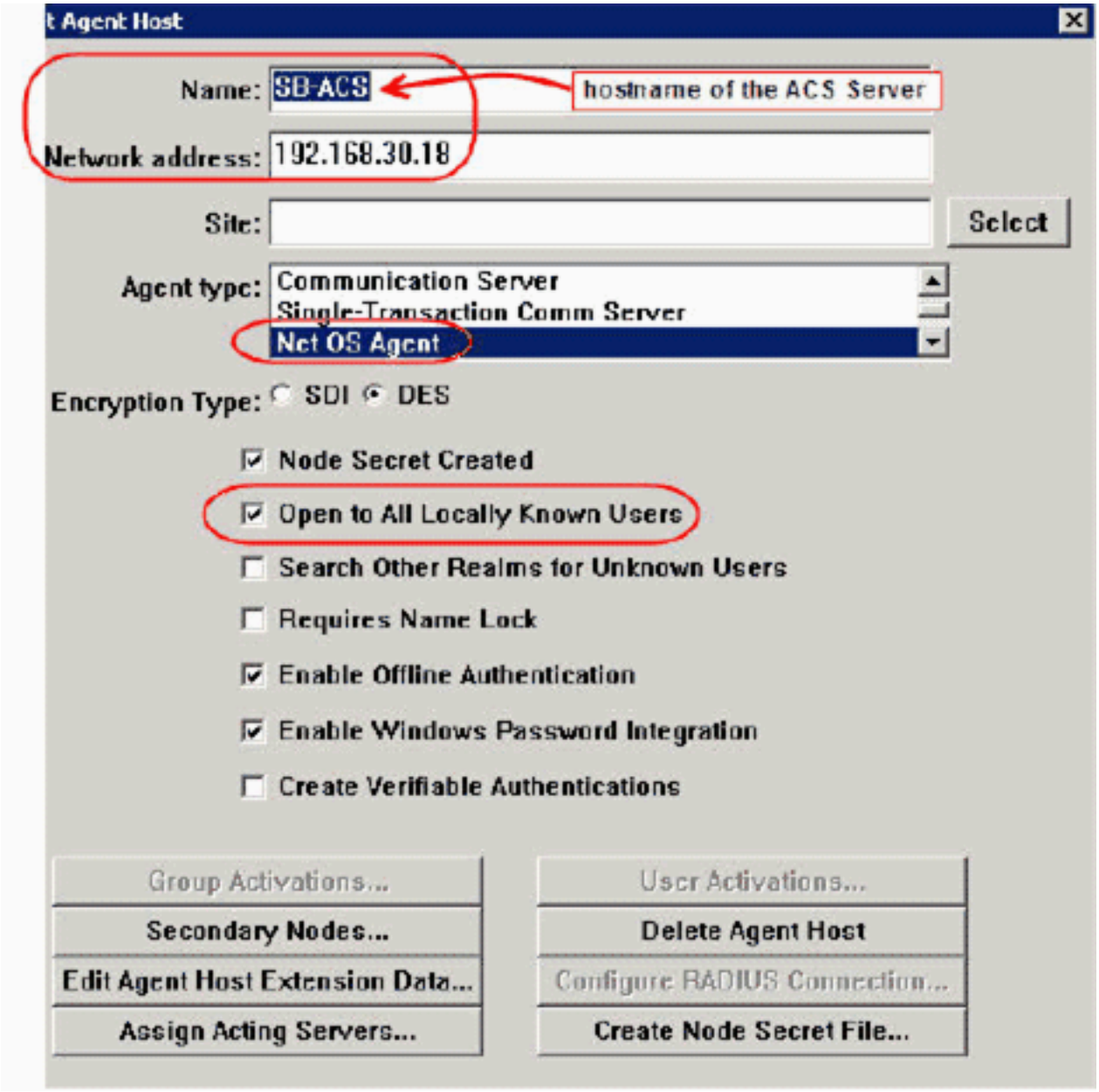
- اسم المضيف لخادم Cisco ACS
- عناوين IP لجميع واجهات الشبكة لخادم ACS من Cisco

أكمل الخطوات التالية:

1. افتح تطبيق وضع مضيف مدير مصادقة RSA.
2. حدد **مضيف الوكيل > إضافة مضيف وكيل**.



ترى هذه النافذة:



3. أدخل المعلومات المناسبة لاسم خادم Cisco ACS وعنوان الشبكة. أختر **NetOS** لنوع العامل وحدد خانة الاختيار **فتح لجميع المستخدمين المعروفين محليا**.
4. وانقر فوق **OK**.

إستخدام خادم RADIUS لمدير مصادقة RSA 6.1

من أجل تسهيل الاتصال بين Cisco WLC ومدير مصادقة RSA، يجب إضافة سجل مضيف وكيل إلى قاعدة بيانات مدير مصادقة RSA وقاعدة بيانات خادم RADIUS. يحدد سجل مضيف الوكيل عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) من Cisco داخل قاعدة البيانات الخاصة به ويحتوي على معلومات حول الاتصال والتشفير.

لإنشاء سجل مضيف الوكيل، تحتاج إلى هذه المعلومات:

- اسم مضيف WLC
- إدارة عنوان من ال WLC
- سر RADIUS، والذي يجب أن يطابق سر RADIUS على Cisco WLC

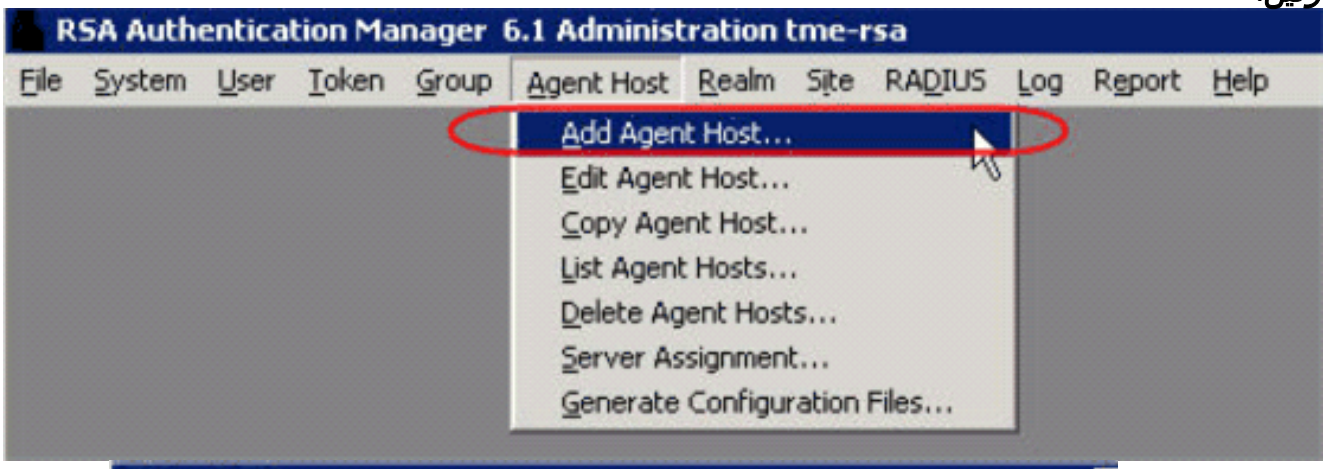
عند إضافة سجل مضيف الوكيل، يتم تكوين دور WLC كخادم إتصالات. يتم إستخدام هذا الإعداد من قبل إدارة مصادقة RSA لتحديد كيفية حدوث الاتصال مع عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

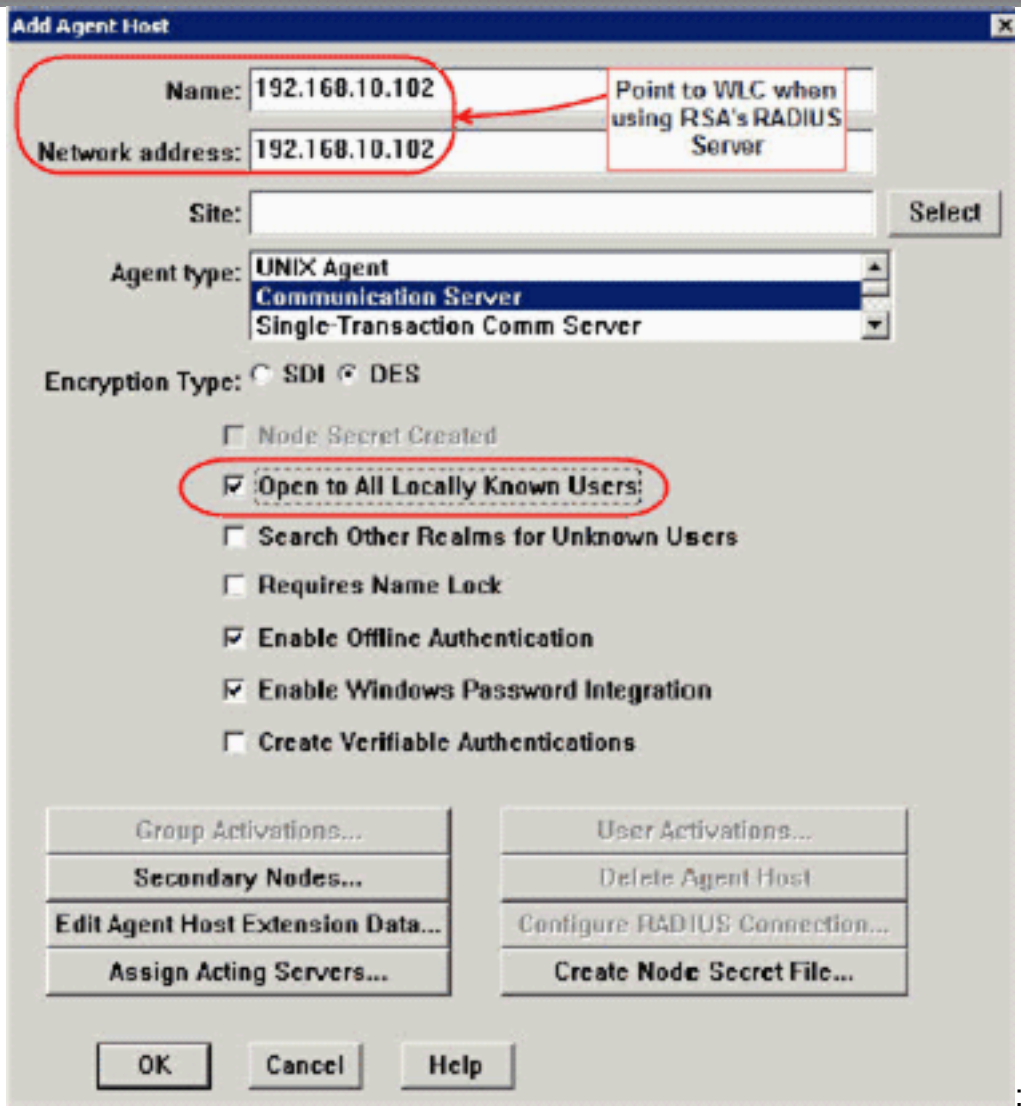
ملاحظة: يجب حل أسماء المضيف داخل إدارة مصادقة RSA / جهاز أمان RSA إلى عناوين IP صالحة على الشبكة

المحلية.

أكمل الخطوات التالية:

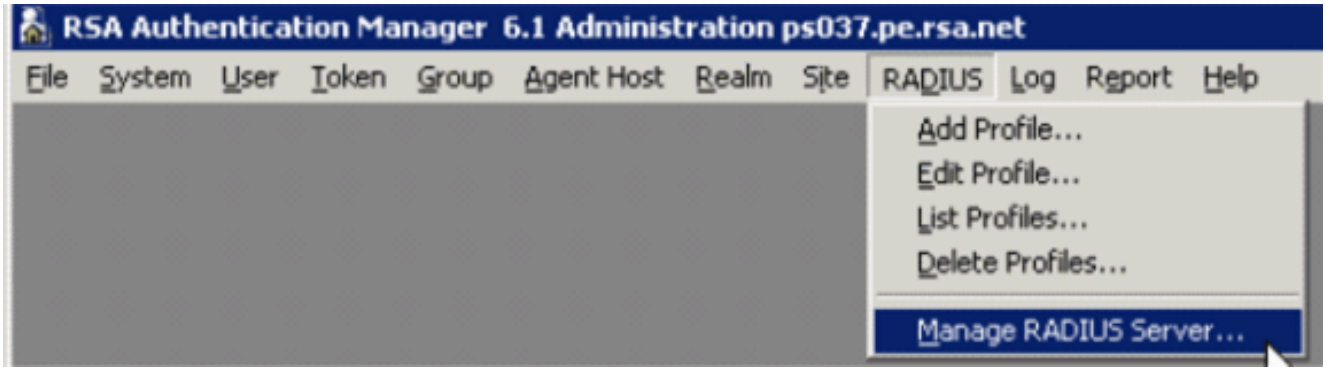
1. افتح تطبيق وضع مضيف مدير مصادقة RSA.
2. حدد **مضيف الوكيل > إضافة مضيف وكيل**.





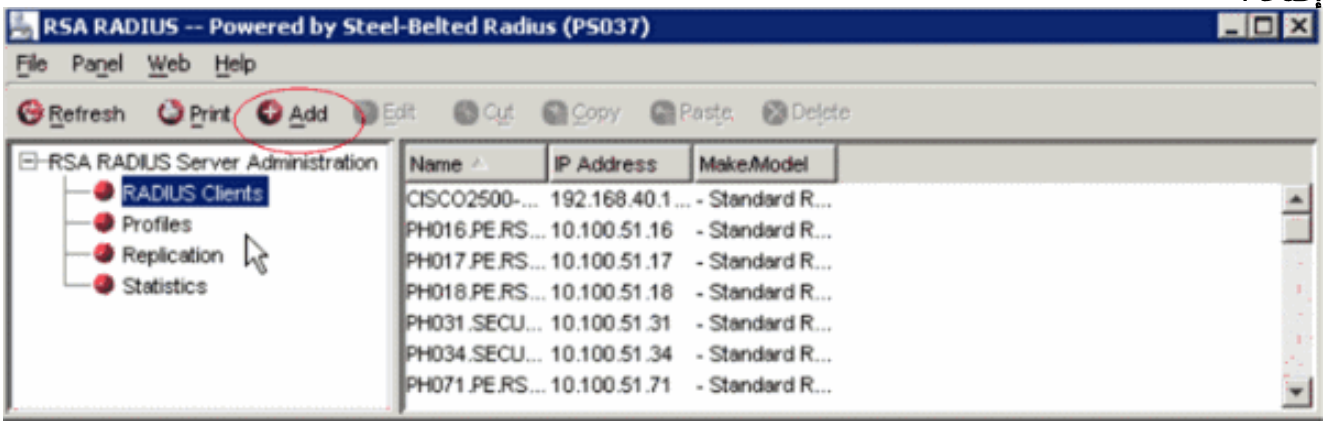
ترى هذه النافذة:

3. أدخل المعلومات المناسبة لاسم مضيف a FQDN) WLC قابل للحل، إذا لزم الأمر) وعنوان الشبكة. أختر **Communication Server** لنوع الوكيل وحدد خانة الاختيار **فتح لجميع المستخدمين المعروفين محليا**.
4. وانقر فوق **OK**.
5. من القائمة، حدد **RADIUS > إدارة خادم RADIUS**.

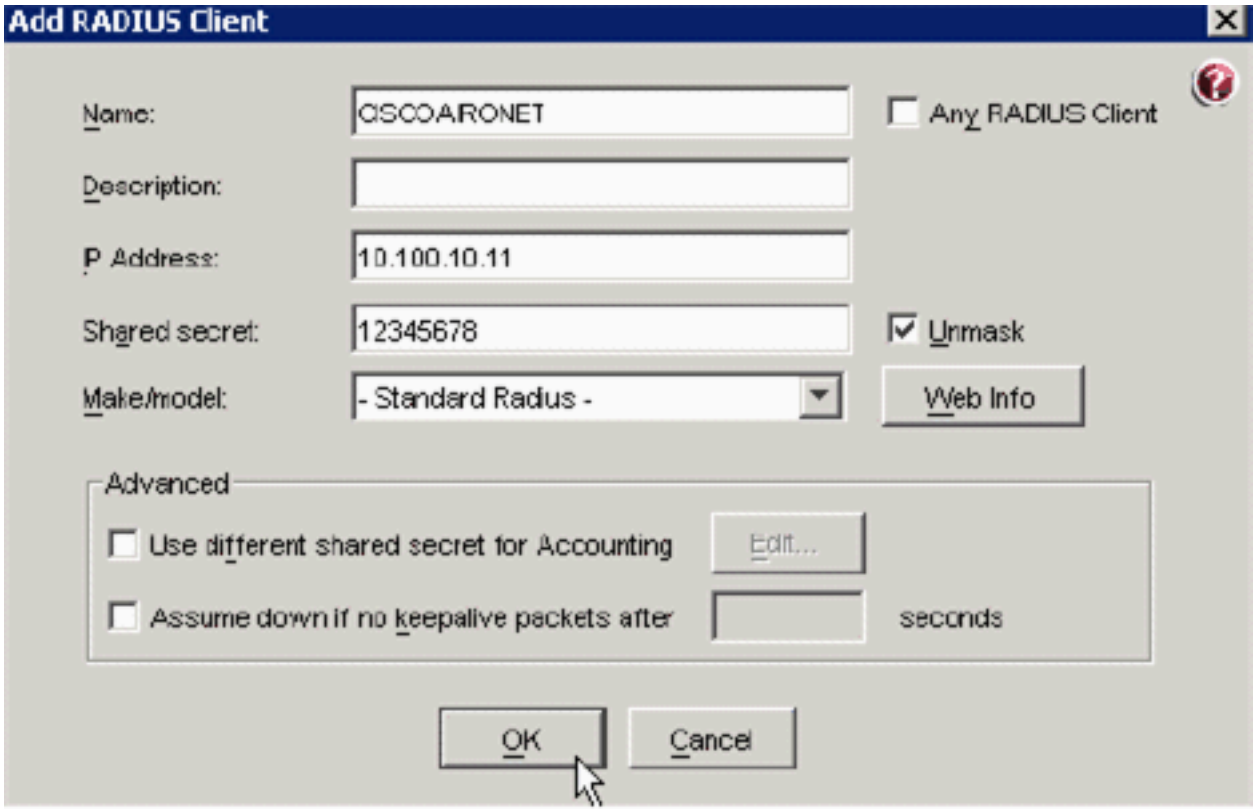


يفتح نافذة إدارة جديد.

6. في هذا الإطار، حدد **عملاء RADIUS**، ثم انقر فوق **إضافة**.



7. دخلت المعلومة مناسب ل ال cisco WLC. يجب أن يطابق السر المشترك السر المشترك المعرف على Cisco WLC.



8. وانقر فوق **OK**.

تكوين وكيل المصادقة

يمثل هذا الجدول وظيفة وكيل مصادقة RSA ل ACS:

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

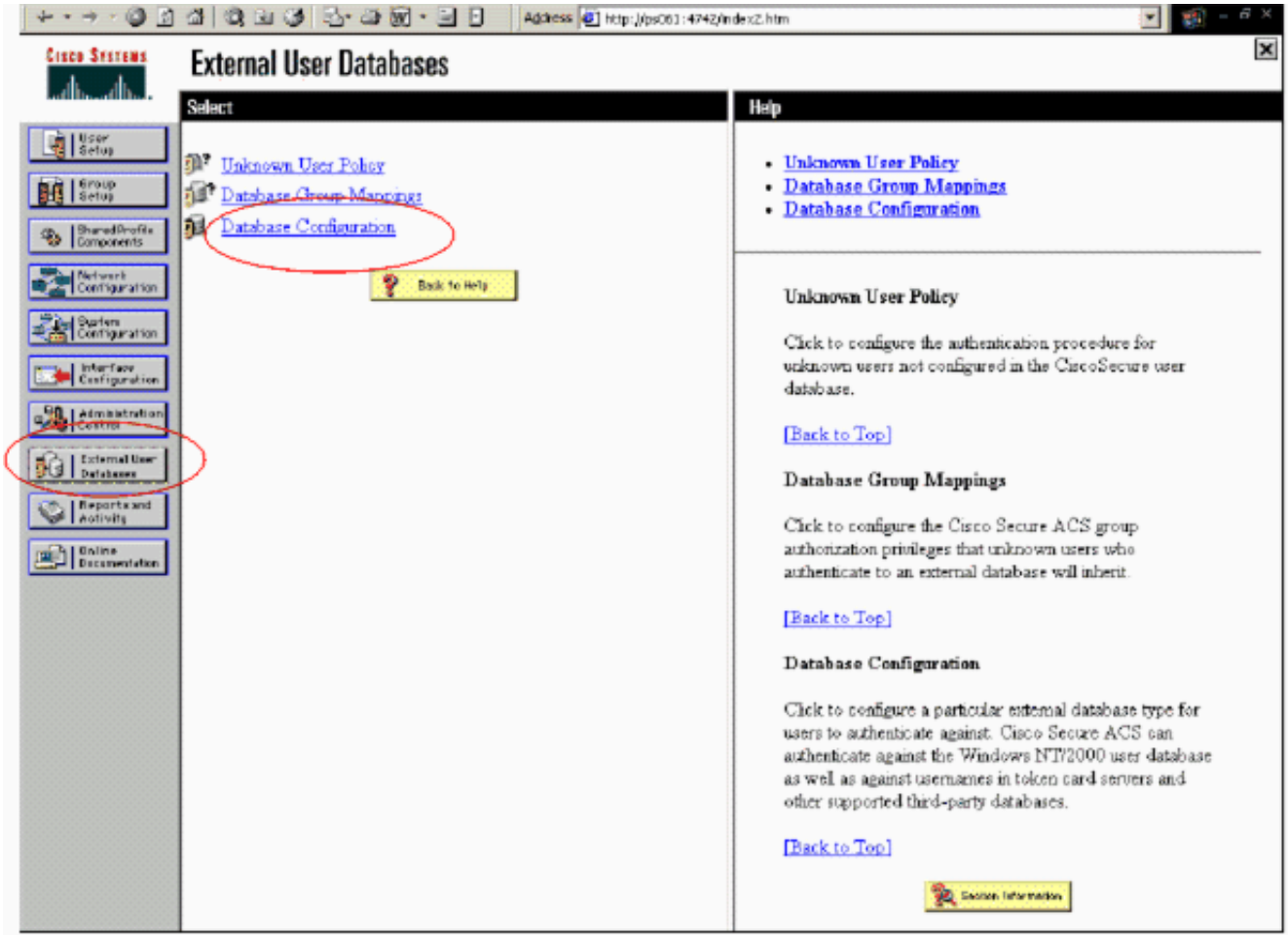
ملاحظة: راجع وثائق RADIUS التي تم تضمينها مع مدير مصادقة RSA حول كيفية تكوين خادم RADIUS، إذا كان ذلك خادم RADIUS الذي سيتم إستخدامه.

تكوين ACS من Cisco

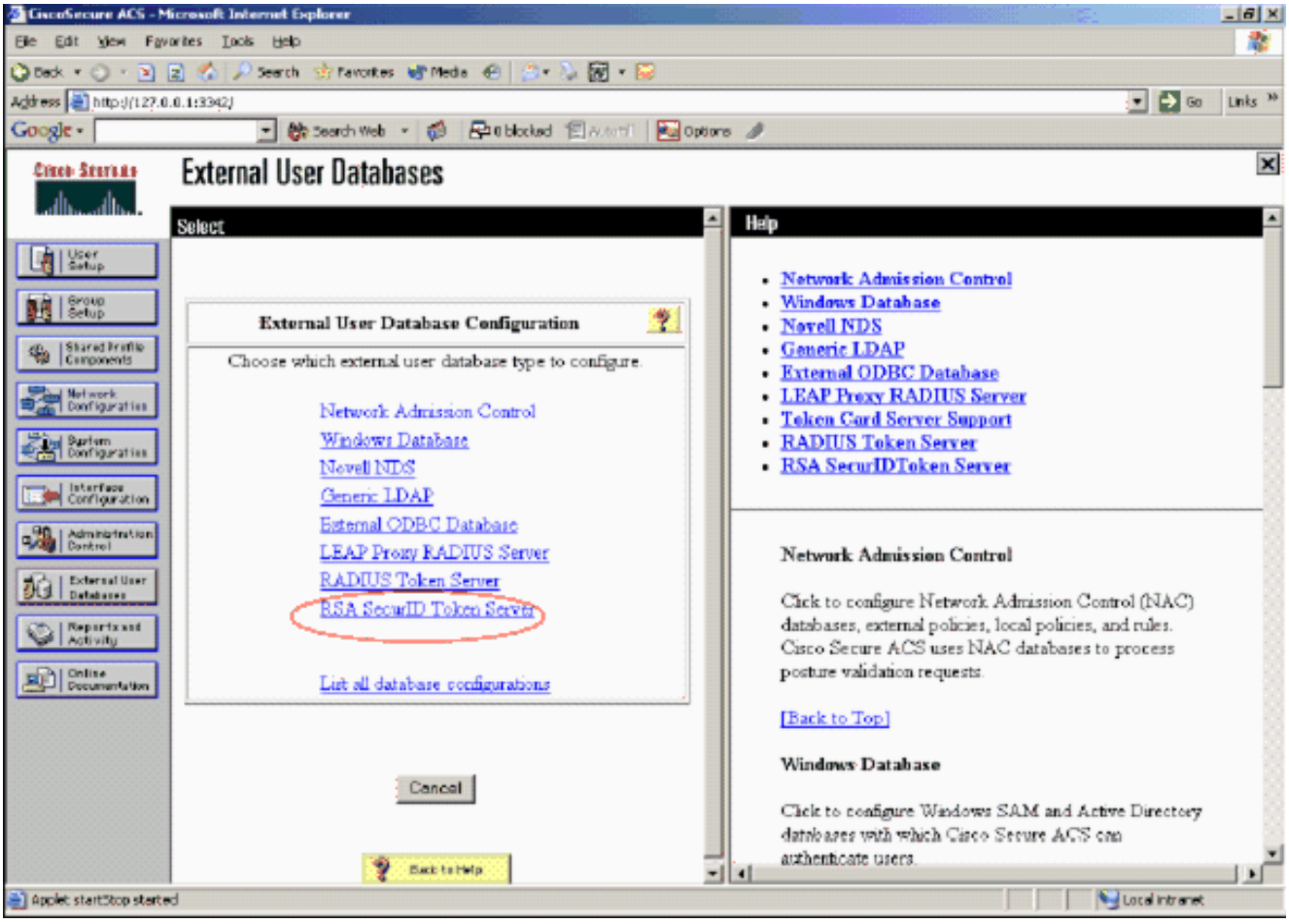
تنشيط مصادقة RSA SecureID

يدعم مصدر المحتوى الإضافي الآمن من Cisco مصادقة RSA SecureID للمستخدمين. أتمت هذا steps in order to شكلت cisco يؤمن ACS أن يصدق مستعمل مع صحة هوية مدير 6.1:

1. قم بتثبيت وكيل مصادقة RSA 5.6 أو إصدار أحدث ل Windows على نفس النظام الخاص بخادم ACS الآمن من Cisco.
2. تحقق من الاتصال من خلال تشغيل وظيفة إختبار المصادقة الخاصة بوكيل المصادقة.
3. انسخ ملف aceclnt.dll من خادم RSA **c:\Program Files\RSA Security\RSA Authentication Manager\prog** Directory إلى **دليل** خادم ACS:**\WINNT\System32**.
4. في شريط التنقل، انقر فوق **قاعدة بيانات المستخدم الخارجي**. ثم انقر فوق **تكوين قاعدة البيانات** في صفحة قاعدة البيانات الخارجية.

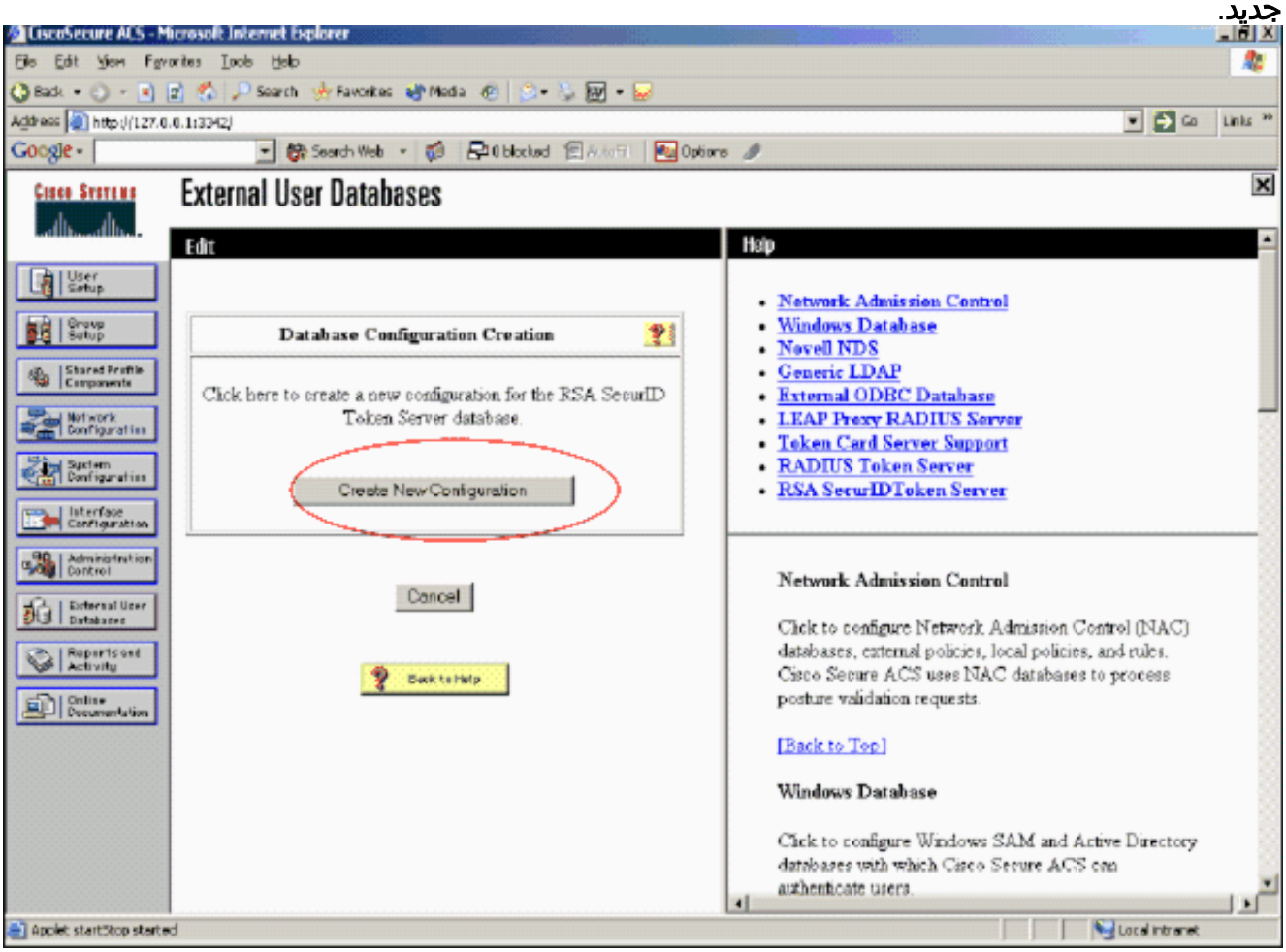


5. في صفحة "تكوين قاعدة بيانات المستخدم الخارجي"، انقر فوق **خادم الرمز المميز RSA SecurID**.

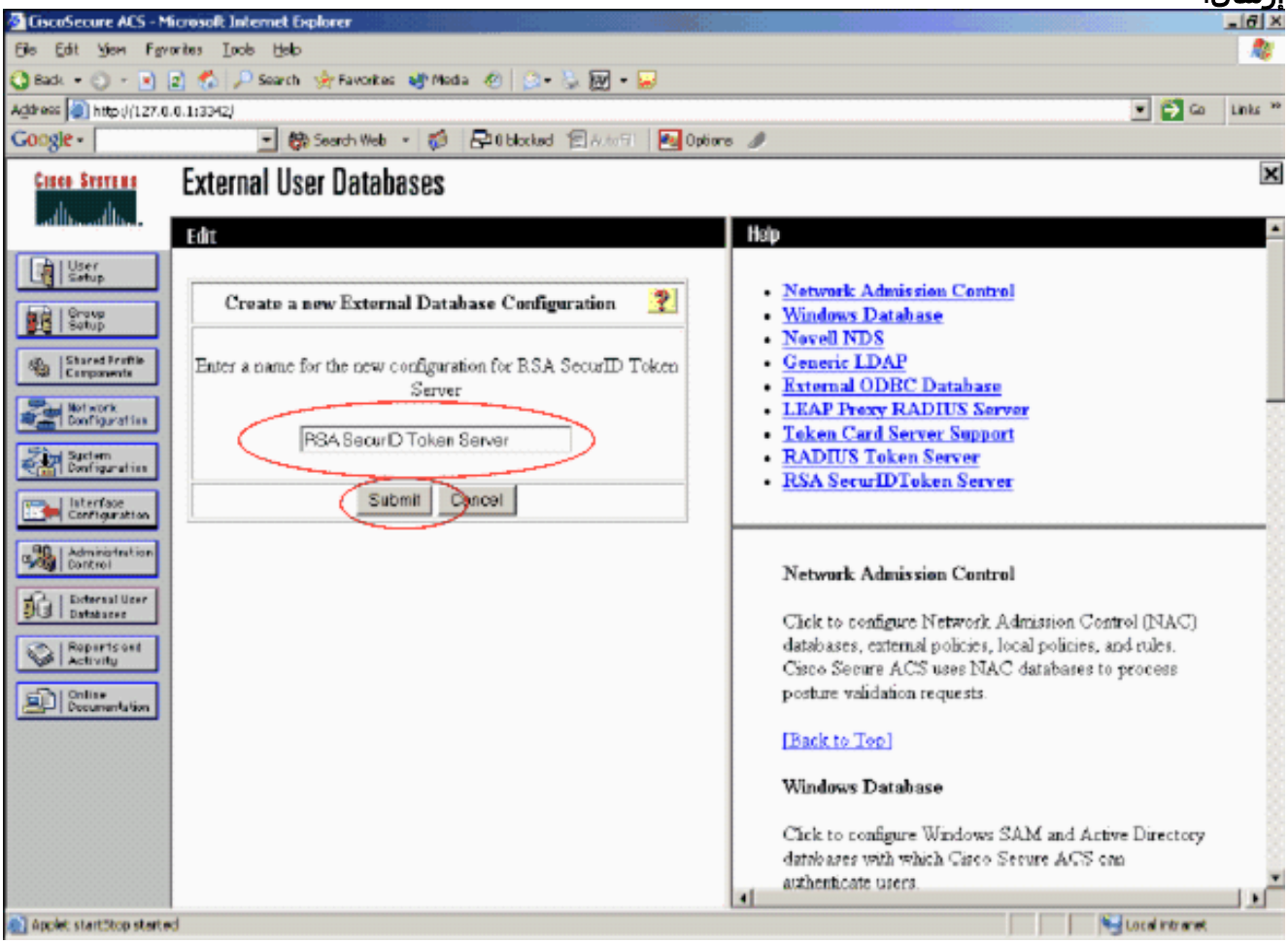


6. طقطقة **يخلق تشكيل**

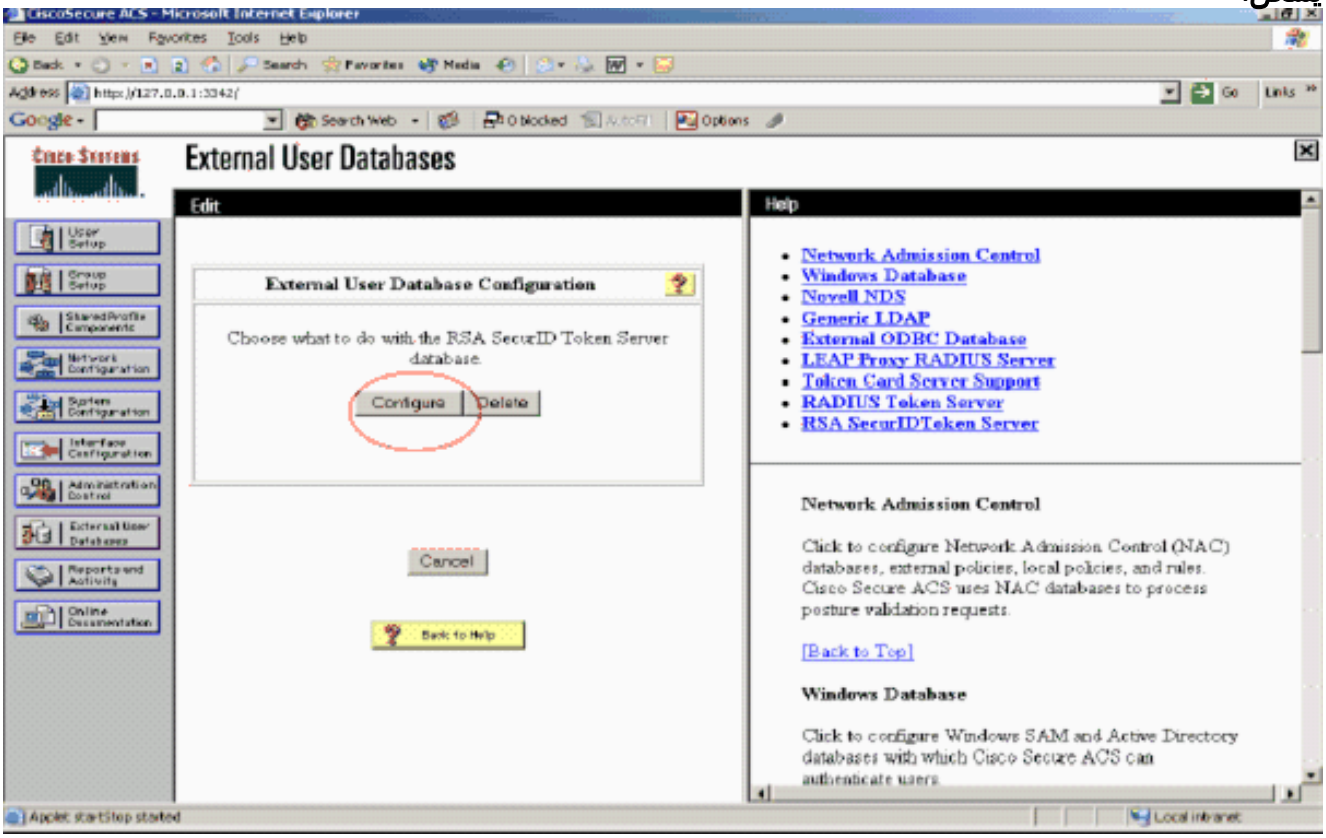
جديد.



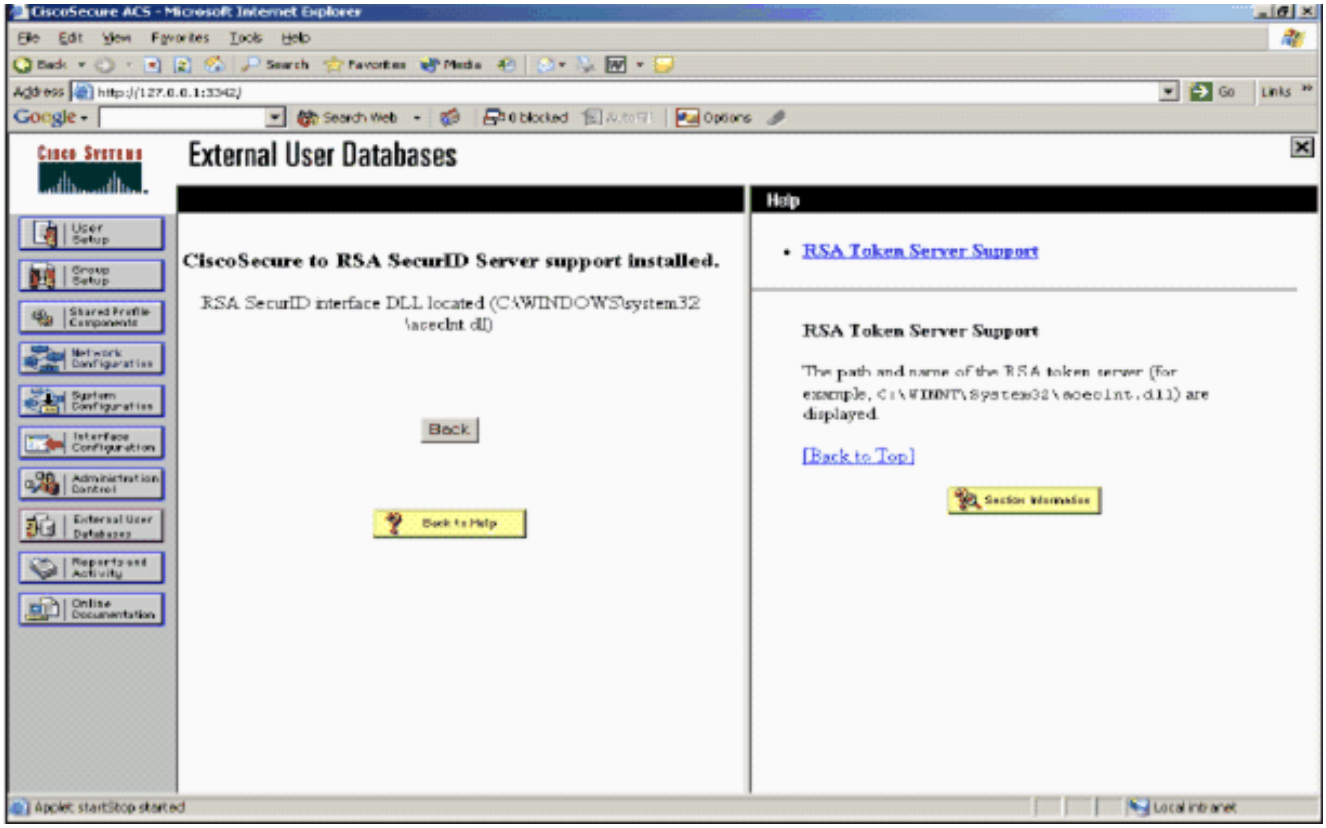
7. أدخل اسما، ثم انقر فوق **إرسال**.



8. طقطقة
يشكل.



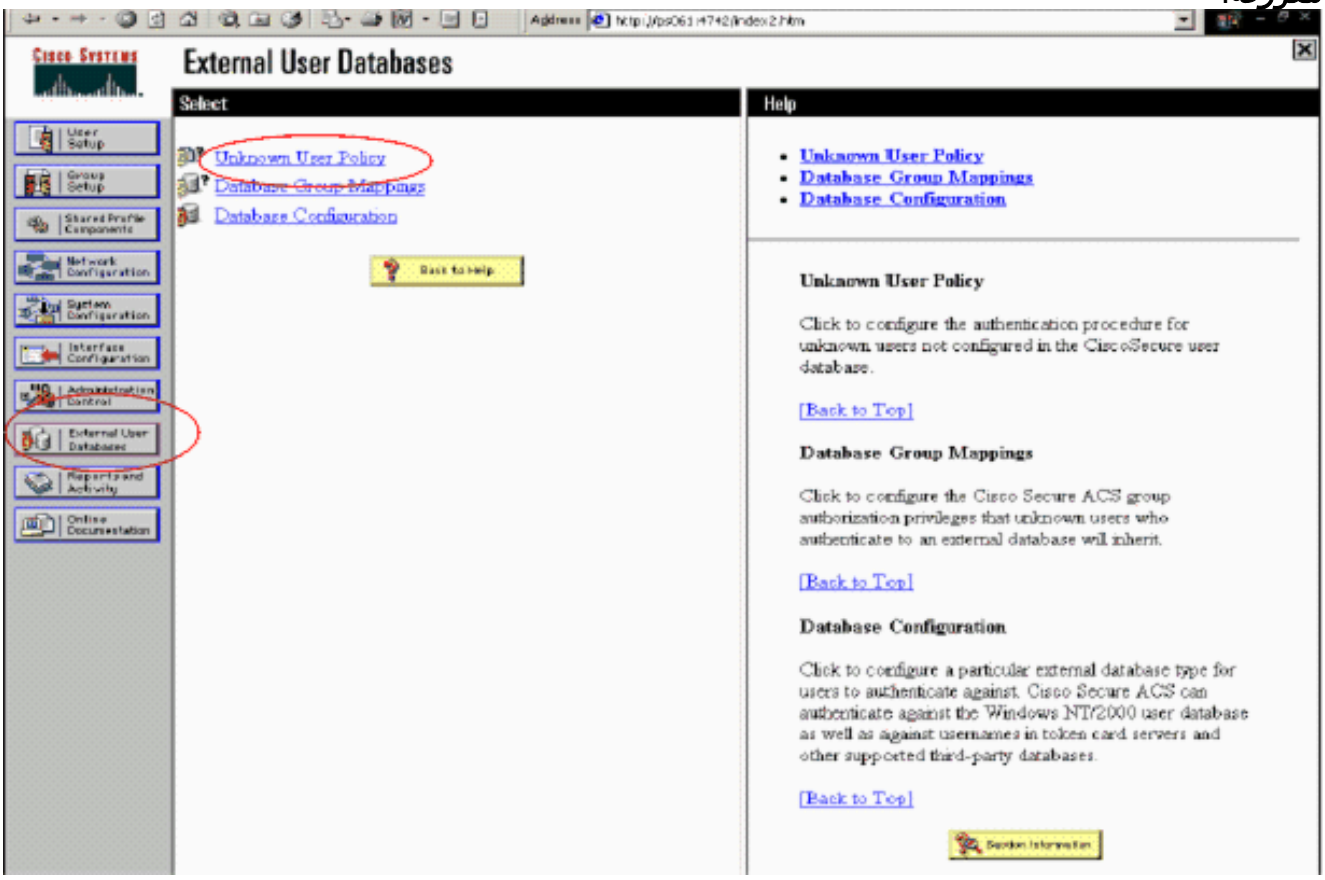
يعرض Cisco Secure ACS اسم خادم الرمز المميز ومسار مكتبة الارتباط الديناميكي (DLL) المصدق. تؤكد هذه المعلومات أنه يمكن ل Cisco Secure ACS الاتصال بوكيل مصادقة RSA. يمكنك إضافة قاعدة بيانات المستخدم الخارجي RSA SecureID إلى نهج المستخدم غير المعروف أو تعيين حسابات مستخدمين معينة لاستخدام قاعدة البيانات هذه للمصادقة.



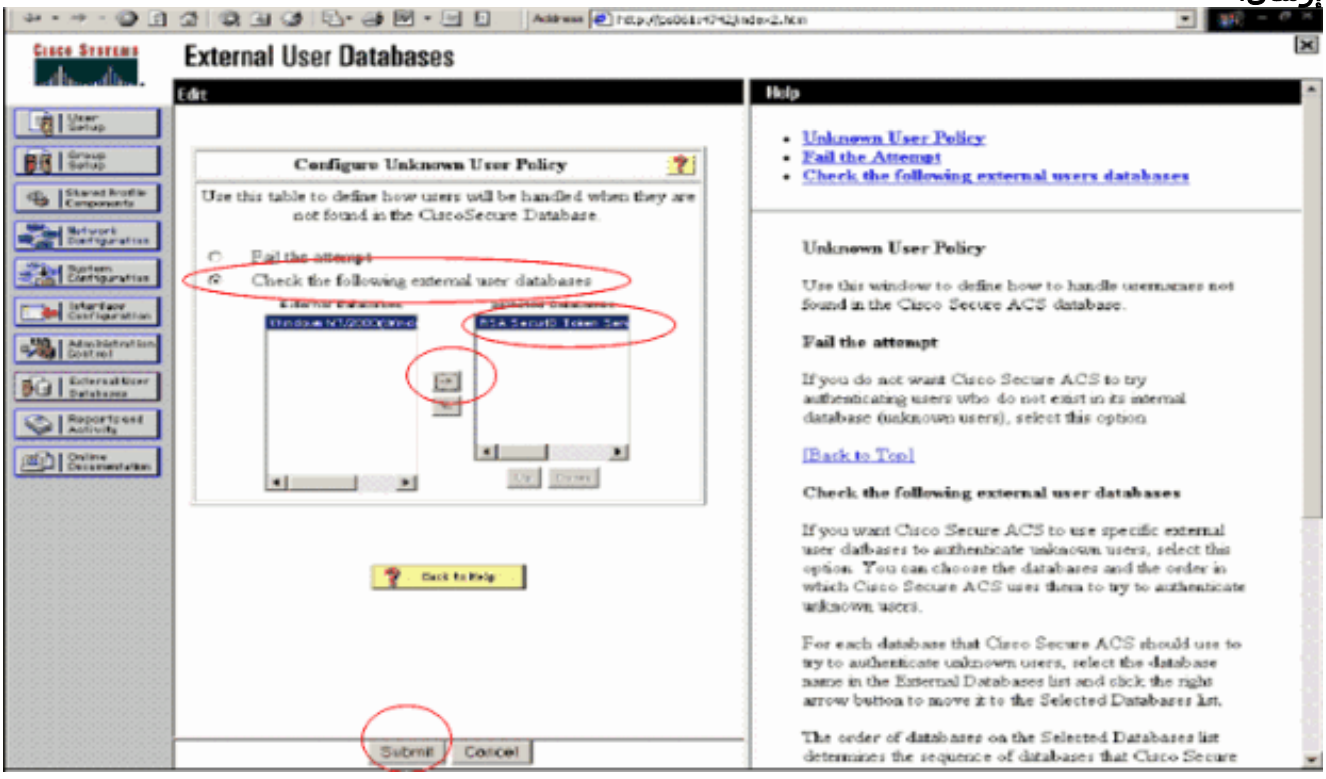
إضافة/تكوين مصادقة RSA SecureID إلى نهج المستخدم غير المعروف

أكمل الخطوات التالية:

1. في شريط تنقل ACS، انقر على **قاعدة بيانات المستخدم الخارجي > سياسة مستخدم غير معروفة**.



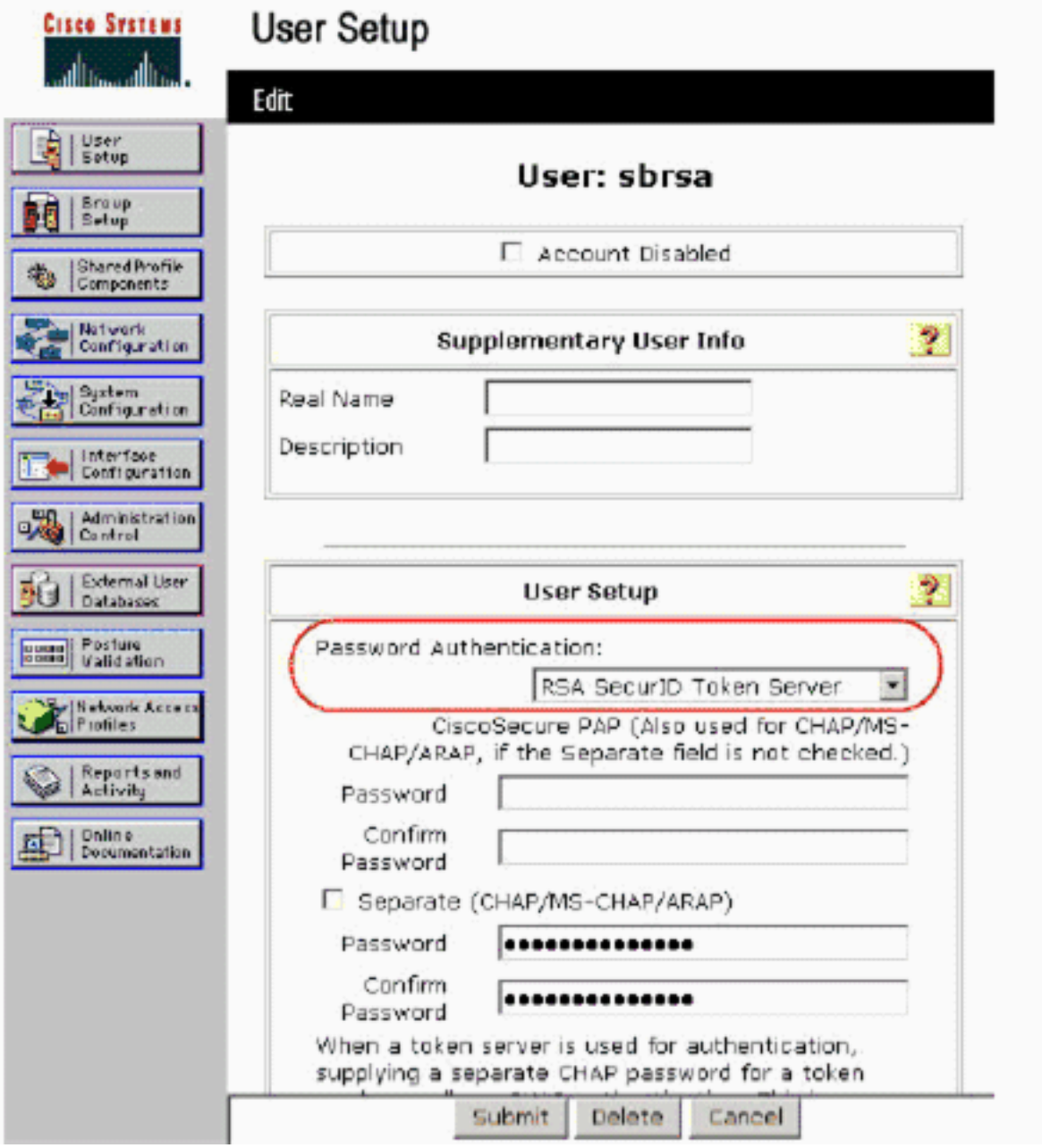
2. في صفحة **نهج المستخدم غير المعروف**، حدد **التحقق من قواعد بيانات المستخدم الخارجية التالية**، وقم بتمييز RSA SecurID Token Server ونقلها إلى مربع قواعد البيانات المحدد. بعد ذلك، انقر فوق **إرسال**.



[إضافة/تكوين مصادقة RSA SecureID لحسابات مستخدمين محددة]

أكمل الخطوات التالية:

1. انقر على **إعداد المستخدم** من واجهة المستخدم الرسومية الرئيسية لمسؤول ACS. أدخل اسم المستخدم وانقر فوق **إضافة** (أو حدد مستخدما موجودا ترغب في تعديله).
2. تحت إعداد المستخدم > مصادقة كلمة المرور، أختر **RSA SecureID Token Server**. بعد ذلك، انقر فوق **إرسال**.

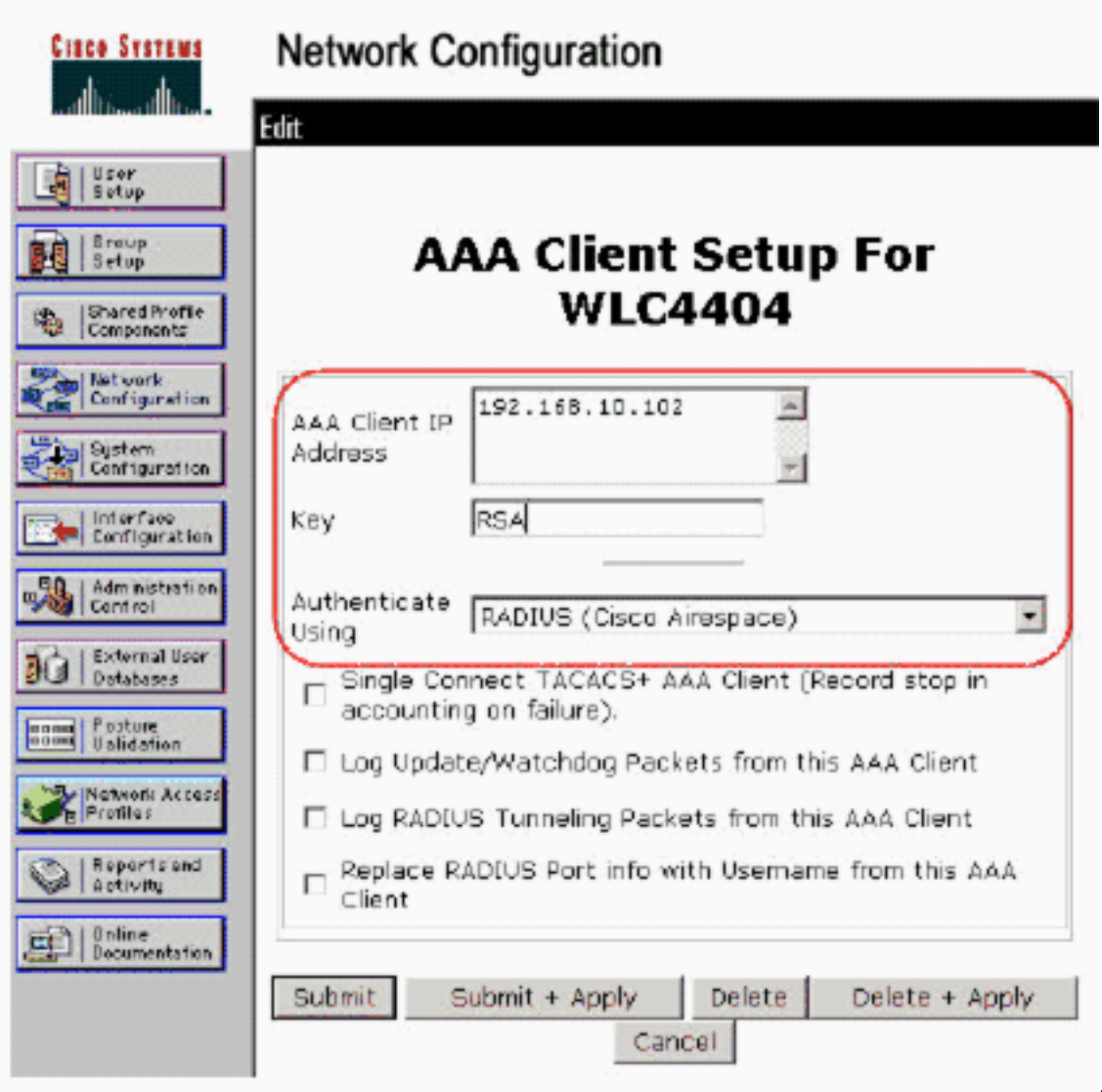


إضافة عميل RADIUS في ACS من Cisco

ستحتاج عملية تثبيت خادم Cisco ACS إلى عناوين IP الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) للعمل كوحدة تخزين متصلة بالشبكة (NAS) لإعادة توجيه مصادقة PEAP الخاصة بالعميل إلى ACS.

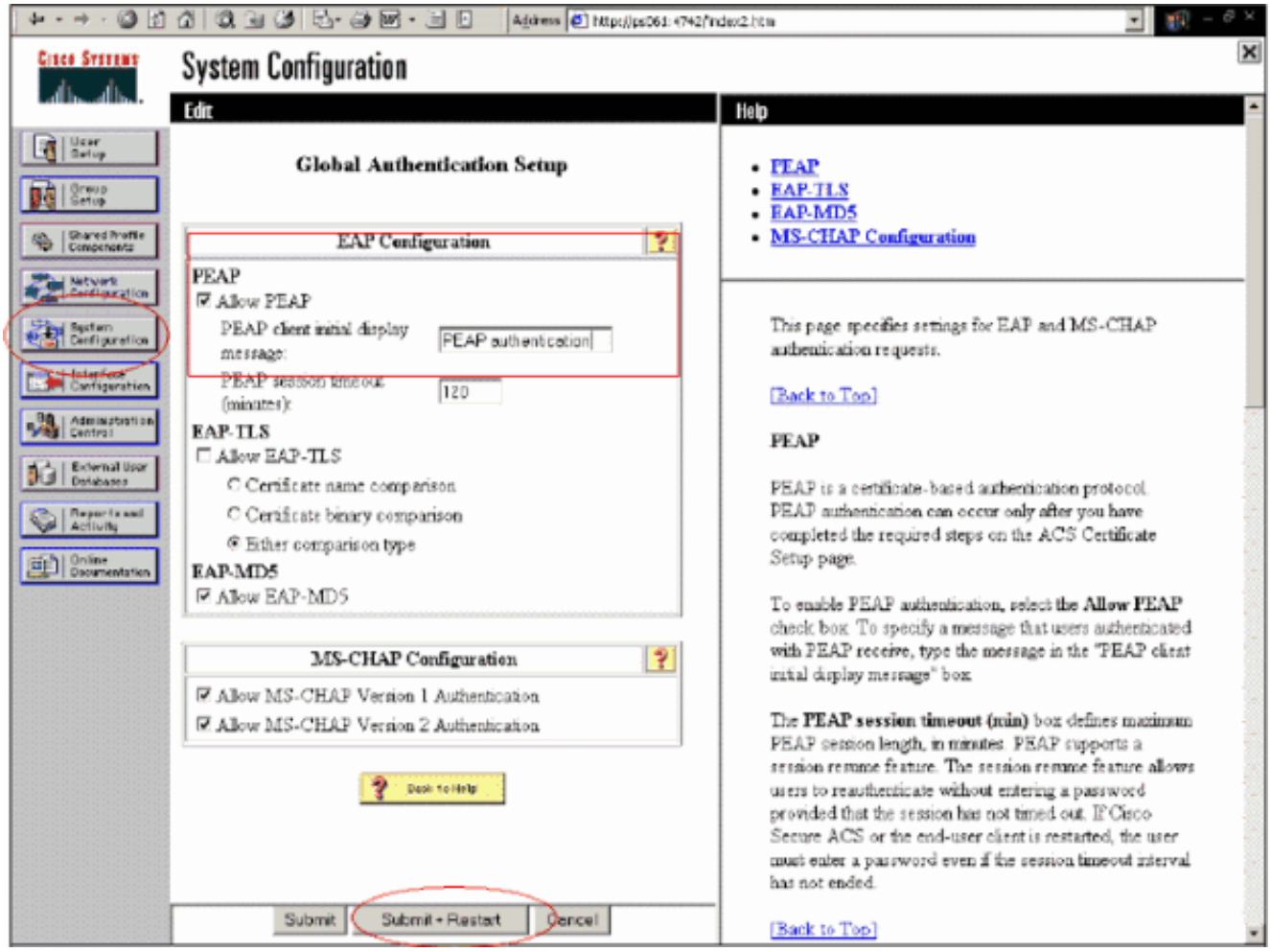
أكمل الخطوات التالية:

1. تحت **تكوين الشبكة**، أضف/حرر عميل AAA ل WLC الذي سيتم إستخدامه. أدخل المفتاح "سري مشترك" (مشترك مع WLC) الذي يتم إستخدامه بين عميل AAA و ACS. حدد **المصادقة باستخدام > RADIUS (Cisco Airespace)** لعميل AAA هذا. ثم انقر فوق **إرسال +**



تطبيق.

2. قدم طلبا لشهادة خادم من مرجع مصدق موثوق به معروف مثل مرجع شهادة RSA Keon وقم بتثبيتها.للحصول على مزيد من المعلومات حول هذه العملية، ارجع إلى الوثائق التي يتم شحنها مع Cisco ACS. إذا كنت تستخدم مدير شهادات RSA، فيمكنك عرض دليل تنفيذ RSA Keon Aironet للحصول على تعليمات إضافية. يجب إكمال هذه المهمة بنجاح قبل المتابعة.**ملاحظة:** يمكن أيضا إستخدام الشهادات الموقعة ذاتيا. ارجع إلى وثائق ACS الآمنة من Cisco حول كيفية إستخدام هذه الملفات.
3. تحت **تشكيل النظام > إعداد المصادقة العامة**، حدد خانة الاختيار **للسماح** بمصادقة PEAP.



تكوين تكوين وحدة تحكم شبكة LAN اللاسلكية من Cisco ل 802.1x

أكمل الخطوات التالية:

1. قم بالاتصال بواجهة سطر الأوامر الخاصة بوحدة التحكم في الشبكة المحلية اللاسلكية (WLC) لتكوين وحدة التحكم حتى يمكن تكوينها للاتصال بخادم ACS الآمن من Cisco.
2. أدخل الأمر **config radius auth ip-address** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتكوين خادم RADIUS للمصادقة.**ملاحظة:** عند الاختبار باستخدام خادم RADIUS لمدير مصادقة RSA، أدخل عنوان IP الخاص بخادم RADIUS لمدير مصادقة RSA. عندما تختبر مع خادم Cisco ACS، أدخل عنوان IP الخاص بخادم ACS الآمن من Cisco.
3. أدخل الأمر **config radius auth port** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتحديد منفذ UDP للمصادقة. تكون المنافذ 1645 أو 1812 نشطة بشكل افتراضي في كل من مدير مصادقة RSA وخادم ACS من Cisco.
4. أدخل الأمر **config radius auth secret** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتكوين السر المشترك على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). يجب أن يتطابق هذا مع السر المشترك الذي تم إنشاؤه في خوادم RADIUS لعميل RADIUS هذا.
5. أدخل الأمر **config radius auth enable** من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لتمكين المصادقة. أدخل الأمر **config radius auth disable** لتعطيل المصادقة عندما ترغب. لاحظ أن المصادقة معطلة بشكل افتراضي.
6. حدد خيار تأمين الطبقة 2 المناسب لشبكة WLAN المطلوبة في عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).
7. أستخدم أوامر **show radius auth statistics** و**show radius summary** للتحقق من تكوين إعدادات RADIUS بشكل صحيح.**ملاحظة:** وحدات التوقيت الافتراضية لمهلة طلب EAP منخفضة وقد تحتاج إلى التعديل. ويمكن القيام بذلك باستخدام الأمر **config advanced eap request-timeout <seconds>**. وقد يساعد أيضا

على تعديل مهلة طلب الهوية بناء على المتطلبات. ويمكن القيام بذلك باستخدام الأمر **config advanced eap** *<seconds>* **identity-request-timeout**.

تكوين العميل اللاسلكي 802.11

للحصول على شرح تفصيلي حول كيفية تكوين أجهزتك اللاسلكية ومطالب العميل، راجع وثائق Cisco المختلفة.

مشكلات معروفة

هذه بعض المشاكل المعروفة جيدا مع مصادقة RSA SecureID:

- رمز برنامج RSA المميز. لا يتم دعم وضع رقم التعريف الشخصي (PIN) الجديد وأوضاع رمز الرمز المميز التالي عند إستخدام هذا النموذج من المصادقة مع XP2. (ثابت كنتيجة ل -ACS-4.0.1-RSA-SW-CSCsc12614 (CSCsd41866.zip
- إذا كان تنفيذ ACS الخاص بك أقدم أو لم يكن لديك التصحيح المذكور أعلاه، فلن يتمكن العميل من المصادقة حتى انتقال المستخدم من "ممكن؛ وضع PIN الجديد" إلى "ممكن". يمكنك تحقيق ذلك من خلال جعل المستخدم يكمل مصادقة غير لاسلكية، أو باستخدام تطبيق "إختبار المصادقة" RSA.
- رفض 4 أرقام / أرقام PIN أبجدية رقمية. إذا كان المستخدم في وضع رقم التعريف الشخصي (PIN) الجديد يتعارض مع نهج رقم التعريف الشخصي (PIN)، فإن عملية المصادقة تفشل، ولا يعلم المستخدم كيف أو لماذا. في العادة، إذا قام المستخدم بمخالفة النهج، فسيتم إرسال رسالة رفض رقم التعريف الشخصي (PIN) وتتم مطالبته مرة أخرى أثناء إظهار نهج رقم التعريف الشخصي (على سبيل المثال، إذا كان نهج رقم التعريف الشخصي (PIN) يتكون من 5 إلى 7 أرقام، يدخل المستخدم 4 أرقام).

معلومات ذات صلة

- تعيين شبكة VLAN الديناميكية مع WLCs استنادا إلى ACS إلى مثال تكوين تعيين مجموعة Active Directory
- شبكة VPN للعميل عبر شبكة LAN اللاسلكية مع مثال تكوين WLC
- المصادقة على أمثلة تكوين وحدات تحكم الشبكة المحلية (LAN) اللاسلكية
- مصادقة EAP-FAST مع وحدات تحكم الشبكة المحلية اللاسلكية ومثال تكوين خادم RADIUS الخارجي
- أنواع المصادقة اللاسلكية على ISR الثابت من خلال مثال تكوين SDM
- أنواع المصادقة اللاسلكية على مثال تكوين ISR الثابت
- بروتوكول المصادقة المتوسع المحمي من Cisco
- مصادقة EAP مع خادم RADIUS
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).