

نم نم آل ا ي فاض إل ا ي و ت ح م ل ا ر د ص م ن ي و ك ت Cisco Windows v3.2 ل ي غ ش ت ل ا م ا ظ ن ل PEAP-MS-CHAPv2 ز ا ه ج ة ق د ا ص م م ا د خ ت س ا ب

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [النظرية الأساسية](#)
- [الاصطلاحات](#)
- [الرسم التخطيطي للشبكة](#)
- [تكوين مصدر المحتوى الإضافي الآمن من Cisco ل Windows v3.2](#)
- [الحصول على شهادة ل خادم ACS](#)
- [تكوين ACS لاستخدام شهادة من التخزين](#)
- [تحديد مراجع الشهادات الإضافية التي يجب أن يثق بها ACS](#)
- [أعد تشغيل الخدمة وشكلت إعدادات PEAP على ACS](#)
- [تحديد نقطة الوصول وتكوينها كعميل AAA](#)
- [تكوين قواعد بيانات المستخدمين الخارجين](#)
- [إعادة تشغيل الخدمة](#)
- [تكوين نقطة وصول Cisco](#)
- [تكوين العميل اللاسلكي](#)
- [تكوين التسجيل التلقائي لجهاز شهادة MS](#)
- [الانضمام إلى المجال](#)
- [تثبيت الشهادة الجذر يدويا على عميل Windows](#)
- [تكوين الشبكة اللاسلكية](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية تكوين بروتوكول المصادقة المتوسع المحمي (PEAP) مع Cisco ACS الآمن ل Windows الإصدار 3.2.

لمزيد من المعلومات حول كيفية تكوين الوصول اللاسلكي الآمن باستخدام وحدات التحكم في الشبكة المحلية اللاسلكية، راجع برنامج Microsoft Windows 2003 و Cisco Secure Access Control Server (ACS) 4.0 تحت PEAP Unified Wireless Networks مع ACS 4.0 و Windows 2003.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية أدناه.

- Cisco Secure ACS ل Windows الإصدار 3.2
 - خدمات شهادات Microsoft (مثبتة كمرجع للشهادات الجذر للمؤسسة [CA]) ملاحظة: للحصول على مزيد من المعلومات، يرجى الرجوع إلى [الدليل المتدرج لإنشاء هيئة تصديق](#) .
 - خدمة DNS مع Windows 2000 Server مع Service Pack 3 ملاحظة: إذا واجهت مشاكل في خادم CA، فقم بتثبيت [الإصلاح العاجل 323172](#) . يتطلب عميل Windows 2000 SP3 [الإصلاح العاجل](#) 313664 لتمكين مصادقة IEEE 802.1x.
 - سلسلة نقاط الوصول اللاسلكية 12.01T من Cisco Aironet 1200
 - الطراز ThinkPad T30 من IBM الذي يعمل بنظام التشغيل Windows XP Professional مع حزمة الخدمة Service Pack 1
- تم إنشاء المعلومات المقدمة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كنت تعمل في شبكة مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر قبل استخدامه.

النظرية الأساسية

يقوم كل من PEAP و EAP-TLS ببناء واستخدام نفق طبقة مأخذ التوصيل الآمنة (TLS) SSL. لا يستخدم PEAP إلا المصادقة من جانب الخادم، والخادم فقط لديه شهادة وثبت هويته للعميل. ومع ذلك يستخدم EAP-TLS المصادقة المتبادلة حيث يمتلك كل من خادم ACS (المصادقة والتحويل والمحاسبة [AAA]) والعملاء شهادات ووثبتون هوياتهم لبعضهم البعض.

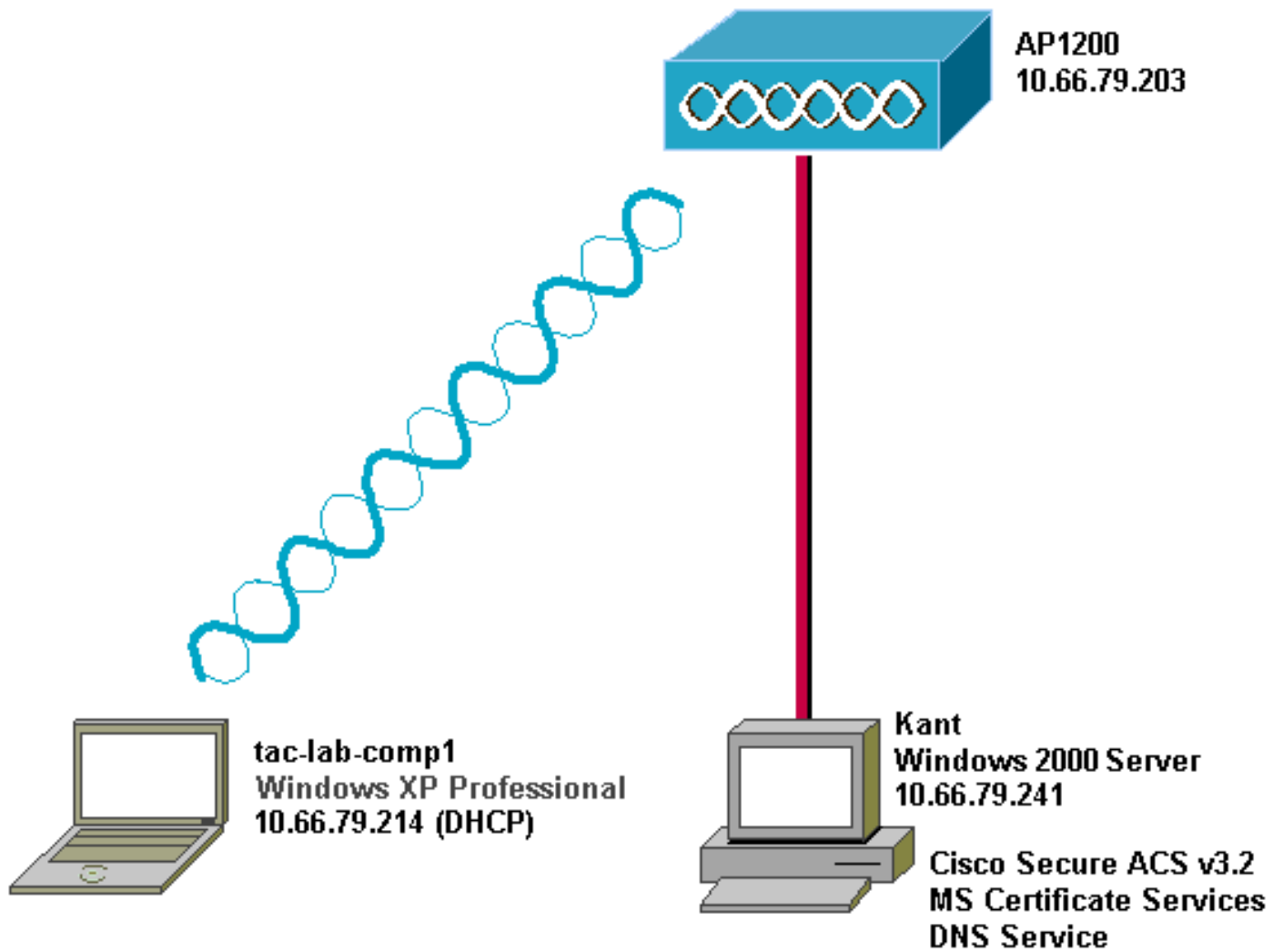
إن PEAP مناسب لأن العملاء لا يطلبون شهادات. يفيد EAP-TLS لمصادقة الأجهزة التي ليس لها رأس، لأن الشهادات تتطلب عدم تفاعل المستخدم.

الاصطلاحات

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في الرسم التخطيطي أدناه.



تكوين مصدر المحتوى الإضافي الآمن من Cisco ل Windows v3.2

اتبع الخطوات التالية لتكوين ACS 3.2.

1. [احصل على شهادة لخادم ACS.](#)
2. [قم بتكوين ACS لاستخدام شهادة من التخزين.](#)
3. [حدد مراجع الشهادات الإضافية التي يجب أن يثق بها ACS.](#)
4. [أعد تشغيل الخدمة وشكلت إعدادات PEAP على ACS.](#)
5. [حدد نقطة الوصول وتكوينها كعمل AAA.](#)
6. [قم بتكوين قواعد بيانات المستخدم الخارجي.](#)
7. [قم بإعادة تشغيل الخدمة.](#)

الحصول على شهادة لخادم ACS

اتبع الخطوات التالية للحصول على الشهادة.

1. على خادم ACS، افتح مستعرض ويب واستعرض إلى خادم CA بإدخال <http://CA-ip-address/certsrv> في شريط العناوين. قم بتسجيل الدخول إلى المجال

Enter Network Password [?] [X]

 Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

Password: *****

Domain: SEC-SYD

Save this password in your password list

OK Cancel

2. حدد طلب شهادة، ثم انقر
كمسؤول.

Microsoft Certificate Services -- Our TAC CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

[Next >](#)

3. حدد طلب متقدم، ثم انقر
التالي.

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

Advanced request

Next >

التالي

4. حدد إرسال طلب شهادة إلى المرجع المصدق هذا باستخدام نموذج، ثم انقر على

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

[Next >](#)

التالي.
5. قم بتكوين خيارات الشهادة. حدد خادم ويب كقالب الشهادة. أدخل اسم خادم

Advanced Certificate Request

Certificate Template:

Identifying Information For Offline Template:

ACS

قم بتعيين حجم المفتاح على 1024. حدد خيارات وضع علامة على المفاتيح كقابلة للتصدير واستخدام مخزن الجهاز المحلي. قم بتكوين خيارات أخرى حسب الحاجة، ثم انقر فوق

Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

- Create new key set
 - Set the container name
- Use existing key set
- Enable strong private key protection
- Mark keys as exportable
 - Export keys to file

Use local machine store

You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm:

Only used to sign request.

Save request to a PKCS #10 file

Attributes:

Submit >

ملا >

إرسال.

ملاحظة: إذا رأيت نافذة تحذير تشير إلى انتهاك للبرمجة النصية (حسب إعدادات الأمان/الخصوصية في المستعرض)، انقر فوق نعم



للمتابعة.

6. انقر على تثبيت هذه

Certificate Issued

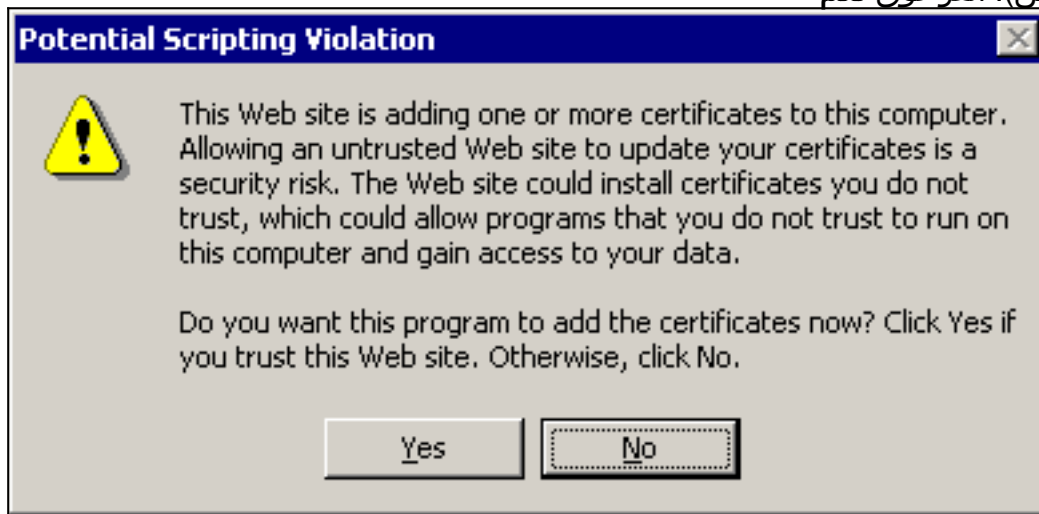
The certificate you requested was issued to you.



[Install this certificate](#)

ملا الشهادة.

حظة: إذا رأيت نافذة تحذير تشير إلى انتهاك للبرمجة النصية (حسب إعدادات الأمان/الخصوصية في المستعرض)، انقر فوق نعم



للمتابعة.

7. في حالة نجاح التثبيت، ستري رسالة

Certificate Installed

Your new certificate has been successfully installed.


تأكيد.

[تكوين ACS لاستخدام شهادة من التخزين](#)

اتبع هذه الخطوات لتكوين ACS لاستخدام الشهادة في التخزين.

1. افتح مستعرض ويب واستعرض إلى خادم ACS بإدخال <http://ACS-ip-address:2002> في شريط العناوين. انقر على تكوين النظام، ثم انقر على إعداد شهادة ACS.
2. انقر على تثبيت شهادة ACS.
3. حدد استخدام شهادة من التخزين. في حقل شهادة CN، أدخل اسم الشهادة التي قمت بتعيينها في الخطوة 5 أ من القسم [احصل على شهادة لخادم ACS](#). انقر على إرسال. يجب أن يتطابق هذا الإدخال مع الاسم الذي كتبتته

في حقل الاسم أثناء طلب الشهادة المتقدمة. هو اسم CN في حقل الموضوع من شهادة الخادم؛ يمكنك تحرير شهادة الخادم للتحقق من هذا الاسم. في هذا المثال، الاسم هو "OurACS". لا تدخل اسم CN الخاص



System Configuration

Edit

Install ACS Certificate

Install new certificate ?

Read certificate from file

Certificate file

Use certificate from storage

Certificate CN

Private key file

Private key password

? Back to Help

Submit Cancel

بالمصدر.
4. عند اكتمال التكوين، ستري رسالة تأكيد تشير إلى تغيير تكوين خادم ACS. ملاحظة: لا تحتاج إلى إعادة تشغيل ACS في هذا

CISCO SYSTEMS

System Configuration

Edit

Install ACS Certificate

Installed Certificate Information ?

Issued to: OurACS
Issued by: Our TAC CA
Valid from: June 23 2003 at 02:19:56
Valid to: June 18 2005 at 00:52:30
Validity: OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install New Certificate Cancel

الوقت.

تحديد مراجع الشهادات الإضافية التي يجب أن يثق بها ACS

وسيق ACS تلقائيا في المراجع المصدق الذي أصدر شهادته الخاصة. إذا تم إصدار شهادات العميل من قبل CAS إضافية، فيجب عليك إكمال الخطوات التالية.

1. انقر على تكوين النظام، ثم انقر على إعداد شهادة ACS.
2. انقر على إعداد مرجع شهادة ACS لإضافة CAS إلى قائمة الشهادات الموثوق بها. في الحقل الخاص بملف شهادة CA، أدخل موقع الشهادة، ثم انقر على

CISCO SYSTEMS

System Configuration

Edit

ACS Certification Authority Setup

CA Operations ?

Add new CA certificate to local certificate storage

CA certificate file

? Back to Help

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

إرسال.
3. انقر على تحرير قائمة الشهادات الموثوق بها. تحقق من كافة الشهادات المصدقة التي يجب على ACS الوثوق بها، وقم بإلغاء تحديد كافة الشهادات المصدقة التي يجب على ACS عدم الثقة بها. انقر على

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

Edit Certificate Trust List

Edit the Certificate Trust List (CTL)

Display Name (Friendly Name)

- ABA.ECOM Root CA
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Naciona
- Baltimore EZ by DST
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B
(CW HKT SecureNet CA Class B)

إرسال

[أعد تشغيل الخدمة وشكلت إعدادات PEAP على ACS](#)

اتبع الخطوات التالية لإعادة تشغيل الخدمة وتشكيل إعدادات PEAP.

1. انقر فوق **تكوين النظام**، ثم انقر فوق **التحكم في الخدمة**.
2. انقر فوق **إعادة التشغيل لإعادة تشغيل الخدمة**.
3. لتكوين إعدادات PEAP، انقر على **تكوين النظام**، ثم انقر على **إعداد المصادقة العامة**.
4. تحقق من الإعدادات الموضحة أدناه، واترك كافة الإعدادات الأخرى كإعدادات افتراضية. إن يريد أنت، أنت يستطيع عينت عملية إعداد إضافي، مثل يمكن إعادة توصيل سريع. عند الانتهاء، انقر فوق **إرسال**. السماح بالإصدار الثاني من بروتوكول EAP-MSCHAPv2 بالسماح بمصادقة MS-CHAP الإصدار 2 ملاحظة: للحصول على مزيد من المعلومات حول الاتصال السريع، ارجع إلى "خيارات تكوين المصادقة" في **تكوين النظام: المصادقة**

ةمچرتل هذه لوج

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