

Windows ل ن م آل ا ي ف ا ض إ ل ا ي و ت ح م ل ا ر د ص م EAP-TLS ز ا ه ج ة ق د ا ص م ع م 3.2 v

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [النظرة 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 EAP-TLS على ACS](#)
- [تحديد نقطة الوصول وتكوينها كعميل AAA](#)
- [تكوين قواعد بيانات المستخدمين الخارجين](#)
- [إعادة تشغيل الخدمة](#)
- [تكوين التسجيل التلقائي لجهاز شهادة MS](#)
- [تكوين نقطة وصول Cisco](#)
- [تكوين العميل اللاسلكي](#)
- [الانضمام إلى المجال](#)
- [الحصول على شهادة للمستخدم](#)
- [تكوين الشبكة اللاسلكية](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تكوين بروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS) باستخدام نظام التحكم في الوصول الآمن (ACS) من Cisco لنظام Windows الإصدار 3.2.

ملاحظة: لا يتم دعم مصادقة الجهاز بواسطة (Novell Certificate Authority (CA). يمكن ل ACS استخدام EAP-TLS لدعم مصادقة الجهاز إلى Microsoft Windows Active Directory. قد يقوم عميل المستخدم النهائي بتحديد بروتوكول مصادقة المستخدم بنفس البروتوكول المستخدم لمصادقة الجهاز. أي أن استخدام EAP-TLS لمصادقة الآلة قد يتطلب استخدام EAP-TLS لمصادقة المستخدم. لمزيد من المعلومات حول مصادقة الجهاز، ارجع إلى قسم [مصادقة الجهاز](#) في دليل المستخدم ل خادم التحكم في الوصول الآمن من Cisco 4.1.

ملاحظة: عند إعداد ACS لمصادقة الأجهزة عبر EAP-TLS وإعداد ACS لمصادقة الجهاز، يجب تكوين العميل لإجراء

مصادقة الجهاز فقط. لمزيد من المعلومات، ارجع إلى كيفية تمكين مصادقة جهاز الكمبيوتر فقط لشبكة قائمة على [802.1X في Windows Vista و Windows Server 2008 و Windows XP Service Pack 3](#).

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 حزمة الخدمة 3 و [Hotfix 323172](#) ملاحظة: إذا واجهت مشاكل في خادم CA، فقم بثبيت [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.

النظرة الأساسية

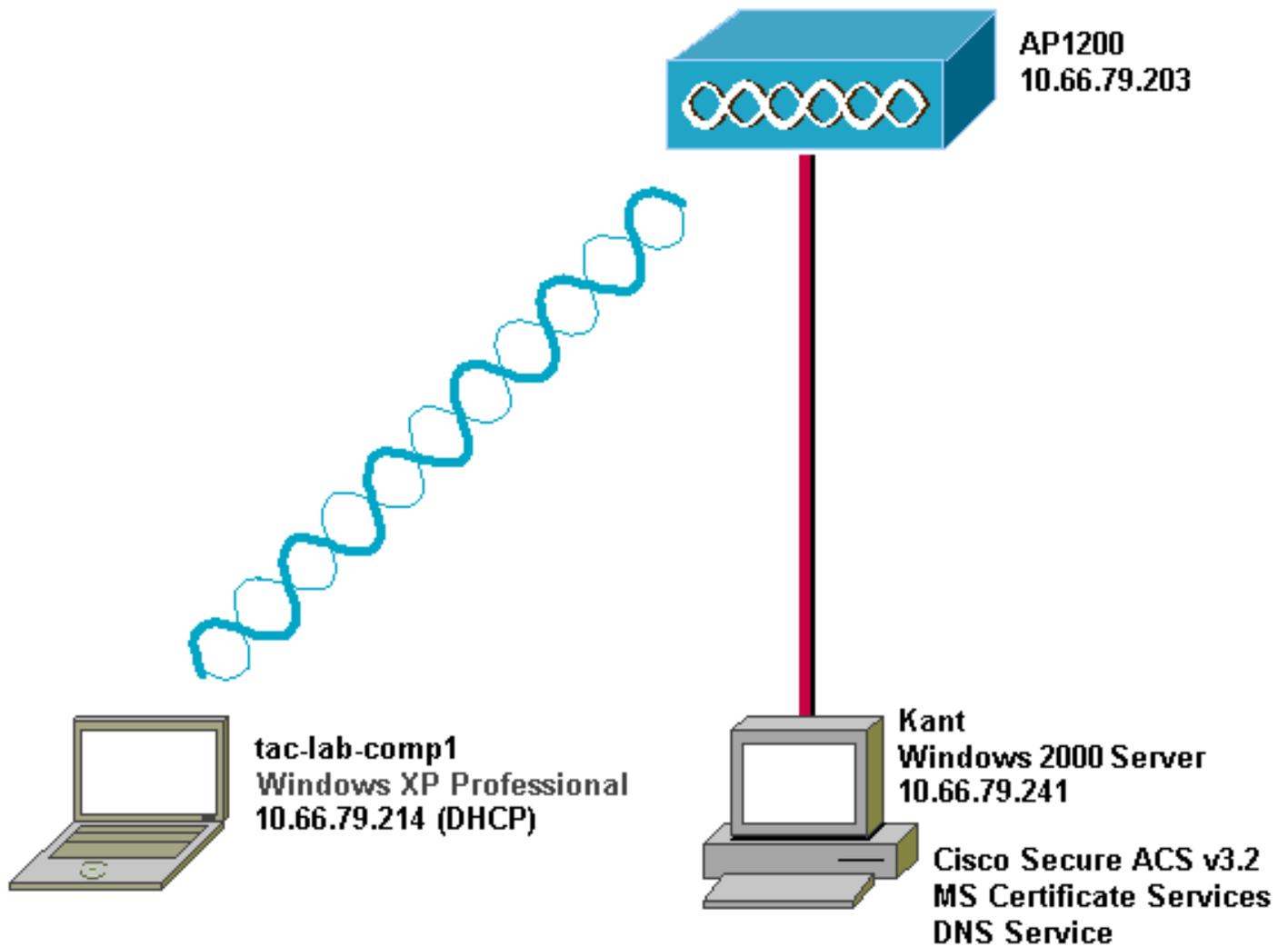
يقوم كل من EAP-TLS وبروتوكول المصادقة المتوسع المحمي (PEAP) بإنشاء نفق طبقة مأخذ التوصيل الآمنة (SSL) واستخدامه. يستخدم EAP-TLS المصادقة المتبادلة حيث يحتوي كل من خادم ACS (المصادقة والتفويض والمحاسبة [AAA]) والعملاء على شهادات وبيئات هوياتهم لبعضهم البعض. إلا أن PEAP لا يستخدم إلا المصادقة من جانب الخادم، والخادم فقط لديه شهادة وبيئات هويته للعميل.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، راجع [اصطلاحات تلميحات 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، وأدخل <http://CA-IP-address/certsrv> للوصول إلى خادم CA.
2. 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

3. 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 >

4. حدد طلب متقدم، ثم انقر
التالي.

Choose Request Type

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

User certificate request:

User Certificate

Advanced request

Next >

التالي

5. 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

6. تكوين خيارات الشهادة: حدد خادم ويب كقالب الشهادة، وأدخل اسم خادم

Advanced Certificate Request

Certificate Template:

Identifying Information For Offline Template:

أدخل

ACS

1024 في حقل "حجم المفتاح"، وحدد مفاتيح العلامة كقابلة للتصدير ثم استخدم خانة الاختيار لمخزن 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.

ظة: إذا ظهرت شاشة انتهاك البرمجة النصية المحتملة، انقر نعم



للمتابعة.

7. انقر على تثبيت هذه

Certificate Issued

The certificate you requested was issued to you.



[Install this certificate](#)

ملأ الشهادة

حظة: إذا ظهرت شاشة انتهاك البرمجة النصية المحتملة، انقر نعم



للمتابعة.

8. في حالة نجاح التثبيت، تظهر رسالة "الشهادة

Certificate Installed

Your new certificate has been successfully installed.

المثبتة."

تكوين ACS لاستخدام شهادة من التخزين

أتمت هذا steps in order to شكلت ACS أن يستعمل الشهادة في تخزين.

1. افتح مستعرض ويب، وأدخل <http://ACS-ip-address:2002> للوصول إلى خادم ACS.
2. انقر على تكوين النظام، ثم انقر على إعداد شهادة ACS.
3. انقر على تثبيت شهادة ACS.
4. انقر على زر استخدام شهادة من راديو التخزين.
5. في حقل شهادة CN، أدخل اسم الشهادة التي قمت بتعيينها في الخطوة 5 أ من [الحصول على شهادة من قسم خادم ACS](#) بهذا المستند.



System Configuration

Edit

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

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

والمجر

إرسال.

د اكمال التكوين، تظهر رسالة تأكيد تشير إلى تغيير تكوين خادم ACS. ملاحظة: لا تحتاج إلى إعادة تشغيل ACS في هذا

CISCO SYSTEMS

System Configuration

Edit

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

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.

الوقت.

تحديد مراجع الشهادات الإضافية التي يجب أن يثق بها ACS

يثق ACS تلقائياً في المرجع 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.
3. 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.

4. انقر على تحرير قائمة الشهادات الموثوق بها.

5. تحقق من كافة الشهادات المصدقة التي يجب على ACS الوثوق بها، وقم بإلغاء تحديد كافة الشهادات المصدقة التي يجب على ACS عدم الثقة بها.

6. 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 EAP-TLS على ACS](#)

أكمل الخطوات التالية لإعادة تشغيل الخدمة وتشكيل إعدادات EAP-TLS:

1. انقر فوق تكوين النظام، ثم انقر فوق التحكم في الخدمة.
2. انقر فوق إعادة التشغيل لإعادة تشغيل الخدمة.
3. طقطقت in order to شكلت EAP-TLS عملية إعداد، نظام تشكيل، وبعد ذلك طقطقت شامل صحة هوية .setup
4. تحقق من السماح ب EAP-TLS، ثم تحقق من واحدة أو أكثر من مقارنات الشهادة.
5. انقر على

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 ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل