

Configurando Cisco asegure ACS para Windows v3.2 con la autenticación de la máquina PEAP-MS-CHAPv2

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Teoría previa](#)

[Convenciones](#)

[Diagrama de la red](#)

[Configure Cisco ACS seguro para Windows v3.2](#)

[Obtenga un certificado para el servidor ACS](#)

[Configure ACS para usar un certificado del almacenamiento](#)

[Especifique autoridades certificadoras adicionales en las que la ACS debe confiar](#)

[Reinicie el servicio y configure PEAP en el ACS](#)

[Especifique y configure el punto de acceso como un cliente AAA](#)

[Configuración de las bases de datos de los usuarios externos](#)

[Reiniciar el servicio](#)

[Configure el Punto de acceso de Cisco](#)

[Configure al cliente de red inalámbrica](#)

[Configure la inscripción automática de la máquina del certificado ms](#)

[Unirse al dominio](#)

[Instale manualmente el certificado raíz en el cliente de Windows](#)

[Configure la comunicación en la red inalámbrica](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento demuestra cómo configurar el protocolo extensible authentication protegido (PEAP) con Cisco ACS seguro para la versión de Windows 3.2.

Para más información sobre cómo configurar el acceso de red inalámbrica seguro usando los reguladores inalámbricos LAN, el software de Microsoft Windows 2003, y el Cisco Secure Access Control Server (ACS) 4.0, refieren al [PEAP bajo redes inalámbricas unificadas con ACS 4.0 y Windows 2003](#).

prerrequisitos

Requisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Cisco ACS seguro para la versión de Windows 3.2
- Servicios de certificado de Microsoft (instalados como Enterprise root certificate authority [CA])**Nota:** [Para obtener más información, consulte la guía paso a paso para configurar una autoridad de certificación.](#)
- El DNS mantiene con Windows 2000 Server con el Service Pack 3**Nota:** [Si experimenta problemas en el Servidor CA, instale hotfix 323172. El cliente del Windows 2000 SP3 requiere el hotfix 313664](#) activar la autenticación del 802.1x de IEEE.
- Unto de acceso de red inalámbrica 12.01T del Cisco Aironet de la serie 1200
- IBM ThinkPad T30 que funciona con al profesional de Windows XP con el Service Pack 1

La Información presentada en este documento fue creada de los dispositivos en un entorno específico del laboratorio. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Teoría previa

El PEAP y el EAP-TLS construyen y utilizan un túnel del Socket Layer TLS/Secure (SSL). El PEAP utiliza solamente la autenticación del lado servidor; solamente el servidor tiene un certificado y prueba su identidad al cliente. El EAP-TLS, sin embargo, utiliza la autenticación recíproca en la cual el servidor y los clientes ACS (autenticación, autorización, y [AAA] de las estadísticas) tienen Certificados y prueban sus identidades el uno al otro.

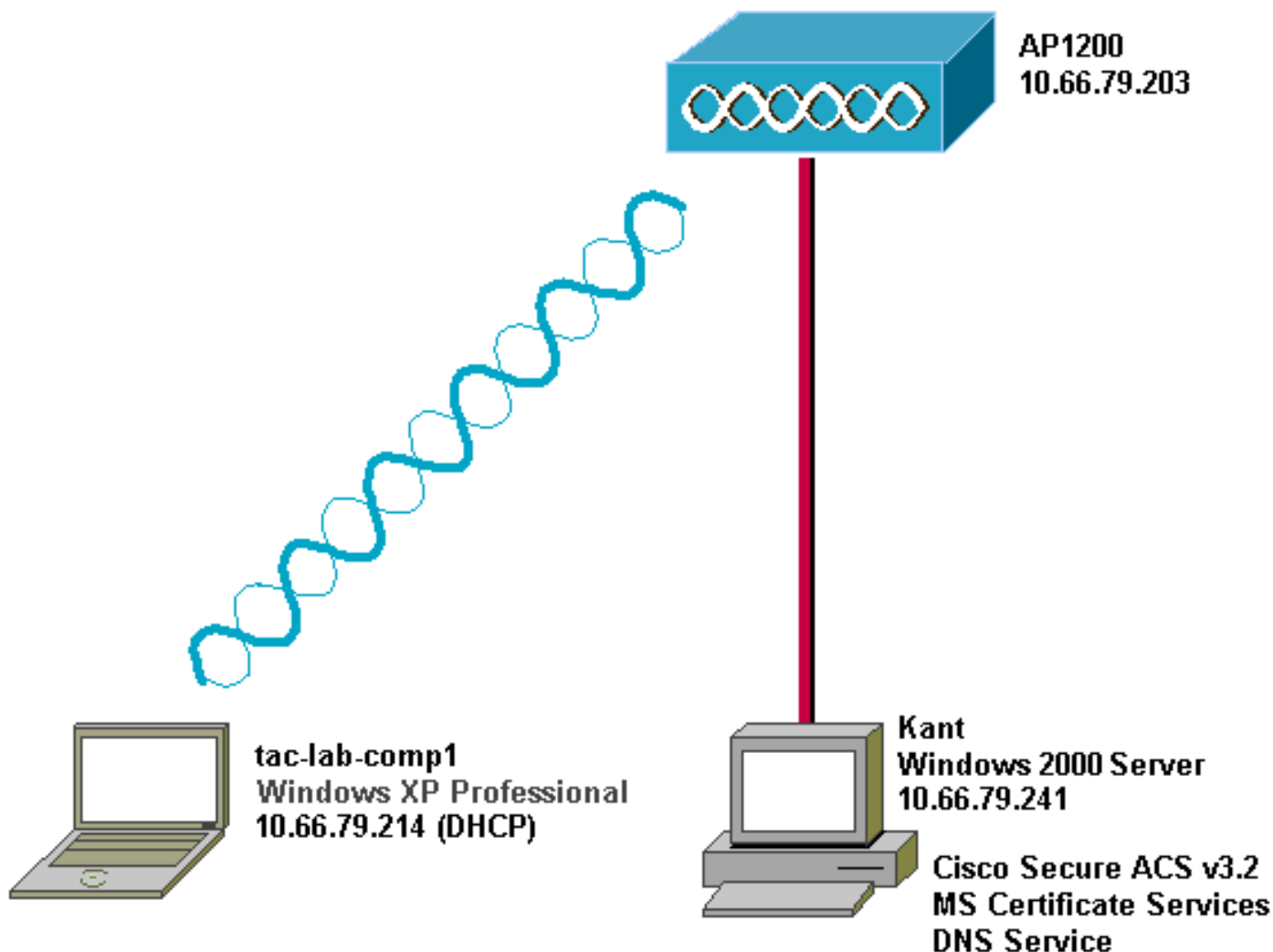
El PEAP es conveniente porque los clientes no requieren los Certificados. El EAP-TLS es útil para autenticar los dispositivos sin encabezado, porque los Certificados no requieren ninguna interacción del usuario.

Convenciones

Para más información sobre los convenios del documento, vea los [convenios de los consejos técnicos de Cisco](#).

Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.



Configure Cisco ACS seguro para Windows v3.2

Siga los siguientes pasos para configurar ACS 3.2.

1. [Obtenga un certificado para el servidor ACS.](#)
2. [Configure el ACS para utilizar un certificado almacenado.](#)
3. [Especifique las autoridades de certificado adicionales en las que debería confiar el ACS](#) (Servidor de control de acceso seguro).
4. [Reinicie el servicio y configure los parámetros de PEAP en ACS.](#)
5. [Especificar y configurar el punto de acceso como un cliente AAA.](#)
6. [Configure las Bases de datos de usuarios externas.](#)
7. [Reiniciar el servicio.](#)

Obtenga un certificado para el servidor ACS

Siga los siguientes pasos para obtener un certificado.

1. En el servidor ACS, abra un explorador de Internet y busque el servidor CA; para ello, introduzca `http://CA-ip-address/certsrv` en la barra de direcciones. Iniciar sesión en el dominio como

Enter Network Password

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

Administrador.

2. Seleccione la **petición un certificado**, y después haga clic **después**.

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. Seleccione Advanced request (Petición avanzada) y luego haga clic en Next (Siguiente).

Choose Request Type

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

User certificate request:

Advanced request

Next >

4. Seleccione Submit a certificate request to this CA using a form (Enviar una petición de certificado a esta CA mediante un formulario) y luego haga clic en Next (Siguiete).

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 >

5. Configure las opciones del certificado. Seleccione Servidor Web como plantilla de certificado.
Ingrese el nombre del servidor

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS
E-Mail:
Company:
Department:
City:
State:
Country/Region: US

ACS.

Esta

blezca el tamaño de clave en 1024. Seleccione las opciones para las claves de marca como exportables y Usar almacenamiento de máquina local. Configure las otras opciones que sean necesarias y luego haga clic en Submit

Key Options:

CSP:

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:

(Enviar).

ota: Si se abre una ventana de advertencia acerca de la falta de cumplimiento de una secuencia de comandos (depende de la configuración de privacidad/seguridad de su navegador), haga clic en Yes (Sí) para




continuar.

6. Haga clic en Install this certificate (Instalar este certificado).

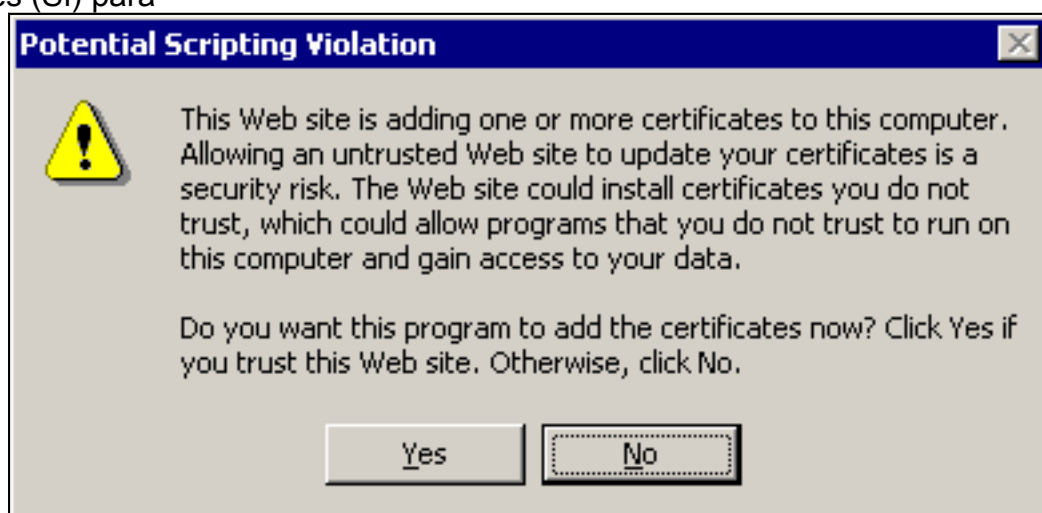
Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

Nota: Si se abre una ventana de advertencia acerca de la falta de cumplimiento de una secuencia de comandos (depende de la configuración de privacidad/seguridad de su navegador), haga clic en Yes (Sí) para



continuar.

7. Si la instalación se ha realizado con éxito, verá un mensaje de confirmación

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

Certificate Installed

Your new certificate has been successfully installed.

[Configure ACS para usar un certificado del almacenamiento](#)

Siga los siguientes pasos para configurar ACS para utilizar el certificado en el almacenamiento.

1. Abra un explorador de Web e ingrese `http://ACS-ip-address:2002/` en la barra de direcciones para buscar el servidor ACS. Haga clic en Configuración del sistema, y luego en Instalación de certificado ACS.
2. El teclado **instala el certificado ACS**.

3. Seleccione Use Certificate from storage (Usar certificado desde almacenamiento). En el campo NC del certificado, ingrese el nombre del certificado que usted asignó en el paso 5a de la sección [obtiene un certificado para el servidor ACS](#). Haga clic en Submit (Enviar). Esta entrada debe hacer juego el nombre que usted pulsó en el campo de nombre durante la solicitud de certificado avanzada. Es el nombre NC en el campo Subject del certificado de servidor; usted puede corregir el certificado de servidor para controlar para saber si hay este nombre. En este ejemplo, el nombre es "OurACS". No ingrese el nombre NC del

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted with a red arrow), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "Edit". Below this is the "Install ACS Certificate" section. A sub-section titled "Install new certificate" contains two radio buttons: "Read certificate from file" (unselected) and "Use certificate from storage" (selected). Below the selected option is a text field labeled "Certificate CN" with the value "OurACS" entered. There are also empty text fields for "Certificate file", "Private key file", and "Private key password". A yellow "Back to Help" button is located below the form. At the bottom of the page are "Submit" and "Cancel" buttons.

emisor.

4. Cuando la configuración haya finalizado, verá un mensaje de confirmación indicando que la configuración del servidor ACS ha sido modificada. **Nota:** No es necesario que reinicie el

The screenshot shows the Cisco Systems logo and the title 'System Configuration'. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled 'Edit' and contains a dialog box for 'Install ACS Certificate'. The dialog box has a tab for 'Installed Certificate Information' with a help icon. The information displayed is: 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, and Validity: OK. Below this is a red warning message: '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.' At the bottom are two buttons: 'Install New Certificate' and 'Cancel'.

ACS ahora.

[Especifique autoridades certificadoras adicionales en las que la ACS debe confiar](#)

El ACS confiará automáticamente en la Autoridad de certificación que emitió su propio certificado. Si los certificados del cliente son publicados por el CAs adicional, después usted necesita completar los pasos siguientes.

1. Haga clic en Configuración del sistema, y luego en Instalación de certificado ACS.
2. Haga clic la **disposición de la autoridad de certificación ACS** para agregar el CAs a la lista de certificados confiables. En el campo para el archivo de certificado CA, ingrese la ubicación del archivo y luego haga clic en Submit

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

(Enviar).

3. El teclado **corrige Certificate Trust List (Lista de confianza del certificado)**. Controle todo el CAs que el ACS debe confiar en, y uncheck todo el CAs que el ACS no debe confiar en. Haga clic en Submit

CISCO SYSTEMS

System Configuration

Edit

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 Nacional
- 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)

(Enviar)

[Reinicie el servicio y configure PEAP en el ACS](#)

Siga los siguientes pasos para recomenzar el servicio y para configurar las configuraciones PEAP.

1. Haga clic en System Configuration (Configuración del sistema), y luego en Service Control (Control del servicio).
2. Haga clic el **reinicio** para recomenzar el servicio.
3. Para configurar las configuraciones PEAP, haga clic la **configuración del sistema**, y después haga clic la **disposición global de la autenticación**.
4. Controle las dos configuraciones mostradas abajo, y deje el resto de las configuraciones como valor por defecto. Si usted desea, usted puede especificar las configuraciones adicionales, tales como permiso rápidamente vuelve a conectar. Cuando haya finalizado, haga clic en Submit (Enviar). **Permita EAP-MSCHAPv2 Permita la autenticación de la versión MS-CHAP 2** **Nota:** Para más información sobre rápido conecte, refiera a las “opciones de configuración de autenticación” en [configuración del sistema: Autenticación y Certificados](#).

