Secure ACS para el v3.2 de Windows con la autenticación de la máquina del EAP-TLS

Contenido

Introducción

Este documento describe cómo configurar el protocolo extensible authentication – Transport Layer Security (EAP-TLS) con el Cisco Secure Access Control System (ACS) para la versión de Windows 3.2.

Nota: La autenticación de la máquina no se soporta con el Certificate Authority (CA) del Novell. El ACS puede utilizar el EAP-TLS para soportar la autenticación de la máquina al Active Directory de Microsoft Windows. El cliente del usuario final pudo limitar el protocolo para la autenticación de usuario al mismo protocolo que se utiliza para la autenticación de la máquina. Es decir, el uso del EAP-TLS para la autenticación de la máquina pudo requerir el uso del EAP-TLS para la autenticación de usuario. Para más información sobre la autenticación de la máquina, refiera a la

sección de la autenticación de la máquina del *guía del usuario para el Cisco Secure Access Control Server 4.1*.

Nota: Cuando configurar el ACS para autenticar las máquinas vía el EAP-TLS y el ACS se ha configurado para la autenticación de la máquina, el cliente se debe configurar para hacer la autenticación de la máquina solamente. Para más información, refiérase cómo habilitar la autenticación de la Computadora-solamente para una red 802.1X-based en Windows Vista, en el Servidor Windows 2008, y en Windows XP Service Pack 3.

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 Secure ACS para la versión 3.2 de Windows
- 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.
- Servicio DNS con Windows 2000 Server con Service Pack 3 y parche 323172**Nota:** Si experimenta problemas en el Servidor CA, instale hotfix 323172. El cliente del Windows 2000 SP3 requiere el hotfix 313664 habilitar la autenticación del IEEE 802.1X.
- Punto de acceso inalámbrico 12.01T de Cisco Aironet de la serie 1200
- Una IBM ThinkPad T30 que ejecuta Windows XP Professional con Service Pack 1

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. 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 Precedente

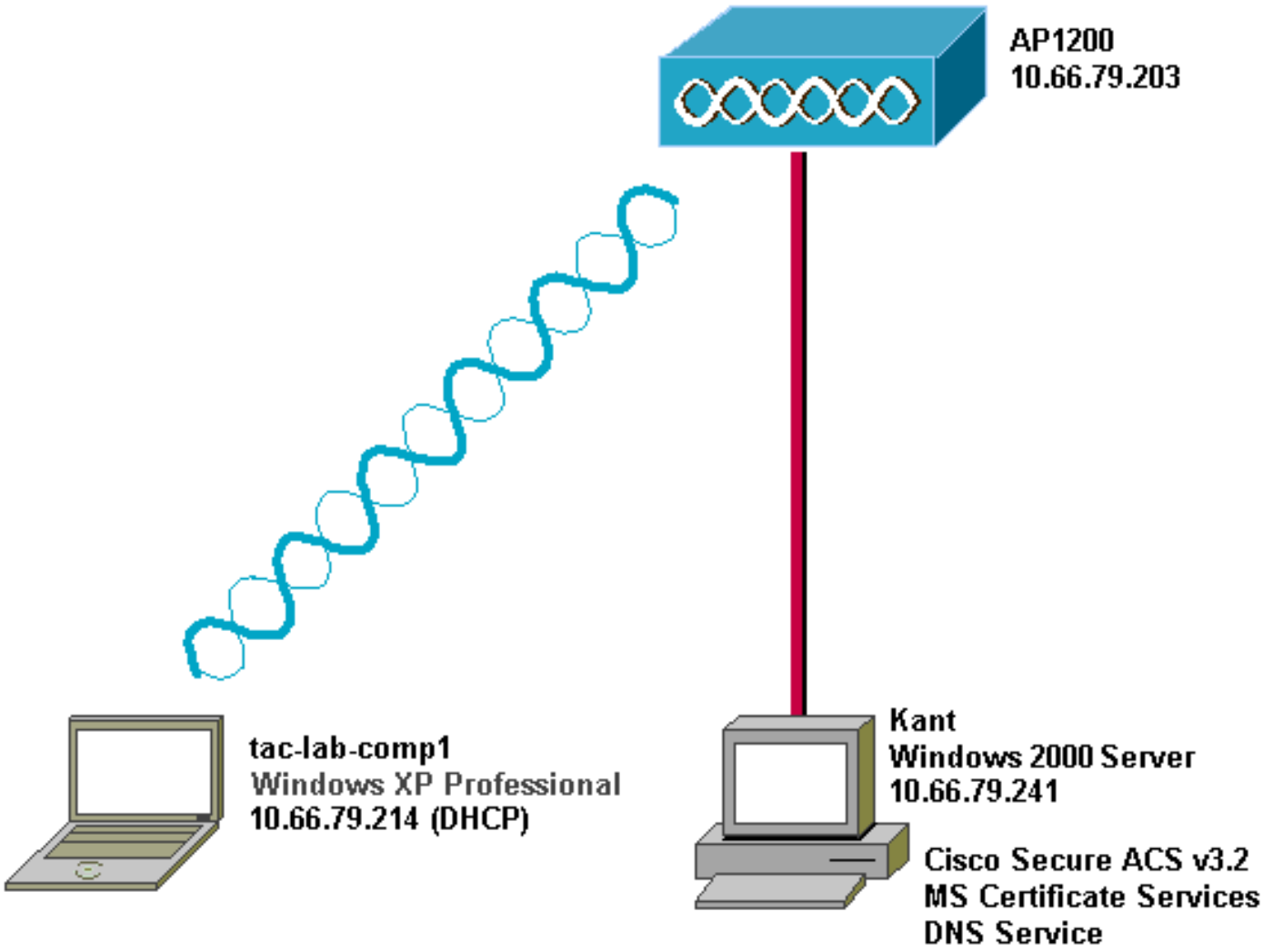
Tanto EAP-TLS como el Protected Extensible Authentication Protocol (PEAP) crean y utilizan un túnel de TLS/Secure Socket Layer (SSL). EAP-TLS usa autenticación mutua en la cual tanto el servidor y los clientes ACS (autenticador, autorizador y contabilizador [AAA]) tienen certificados y confirman sus identidades unos con otros. El PEAP, sin embargo, utiliza solamente la autenticación del lado del servidor; solamente el servidor tiene un certificado y prueba su identidad al cliente.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Diagrama de la red

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



Configuración de Cisco Secure ACS para Windows v3.2

Siga los pasos a continuación 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 los usuarios externos
7. Reiniciar el servicio.

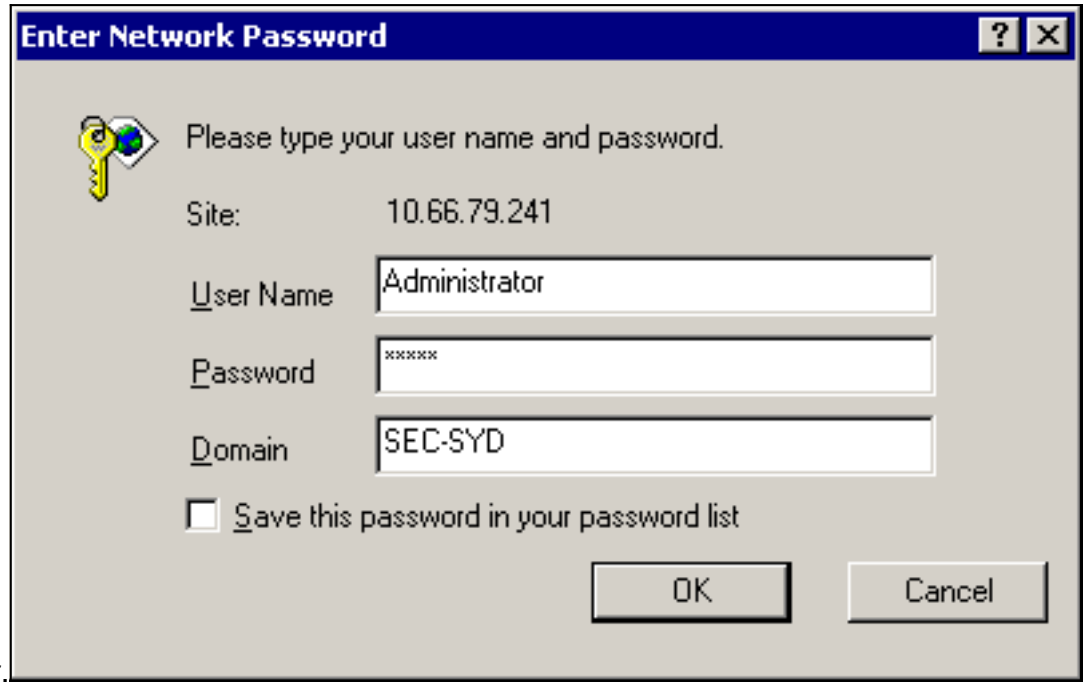
Obtenga un certificado para el servidor ACS

Siga los pasos a continuación para obtener un certificado.

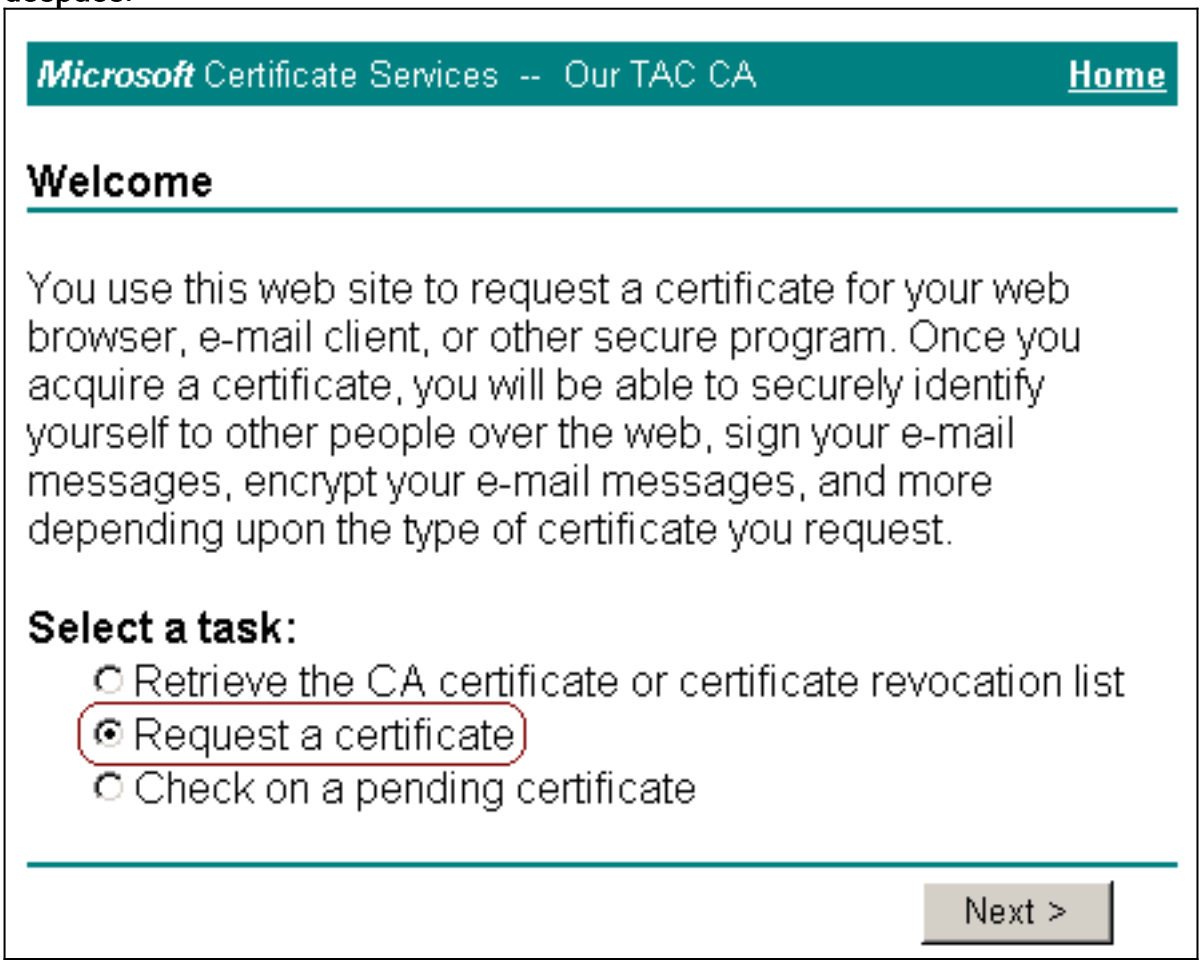
1. En el servidor ACS, abra a un buscador Web, y ingrese **http:// CA-ip-address/certsrv** para

acceder el servidor CA.

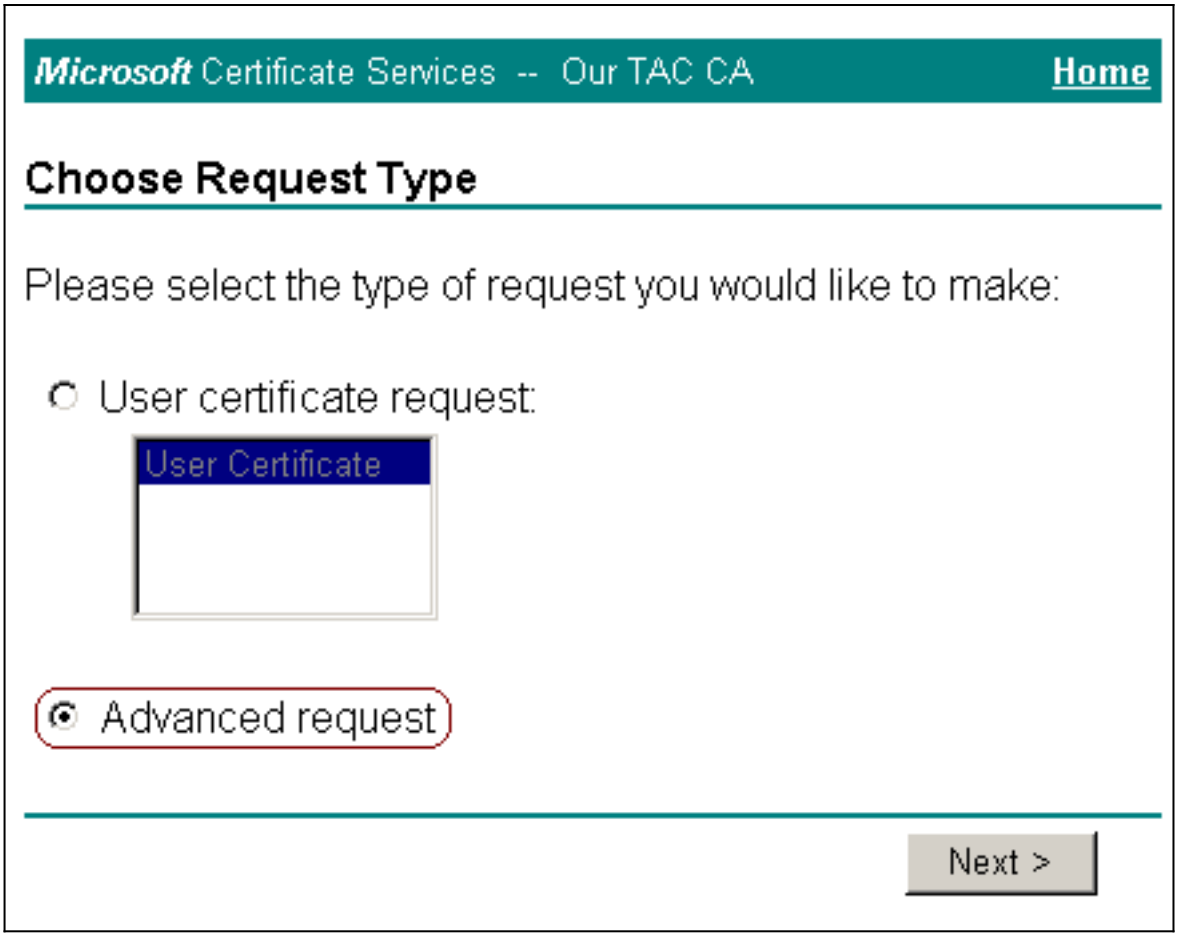
2. Iniciar sesión en el dominio como Administrador.



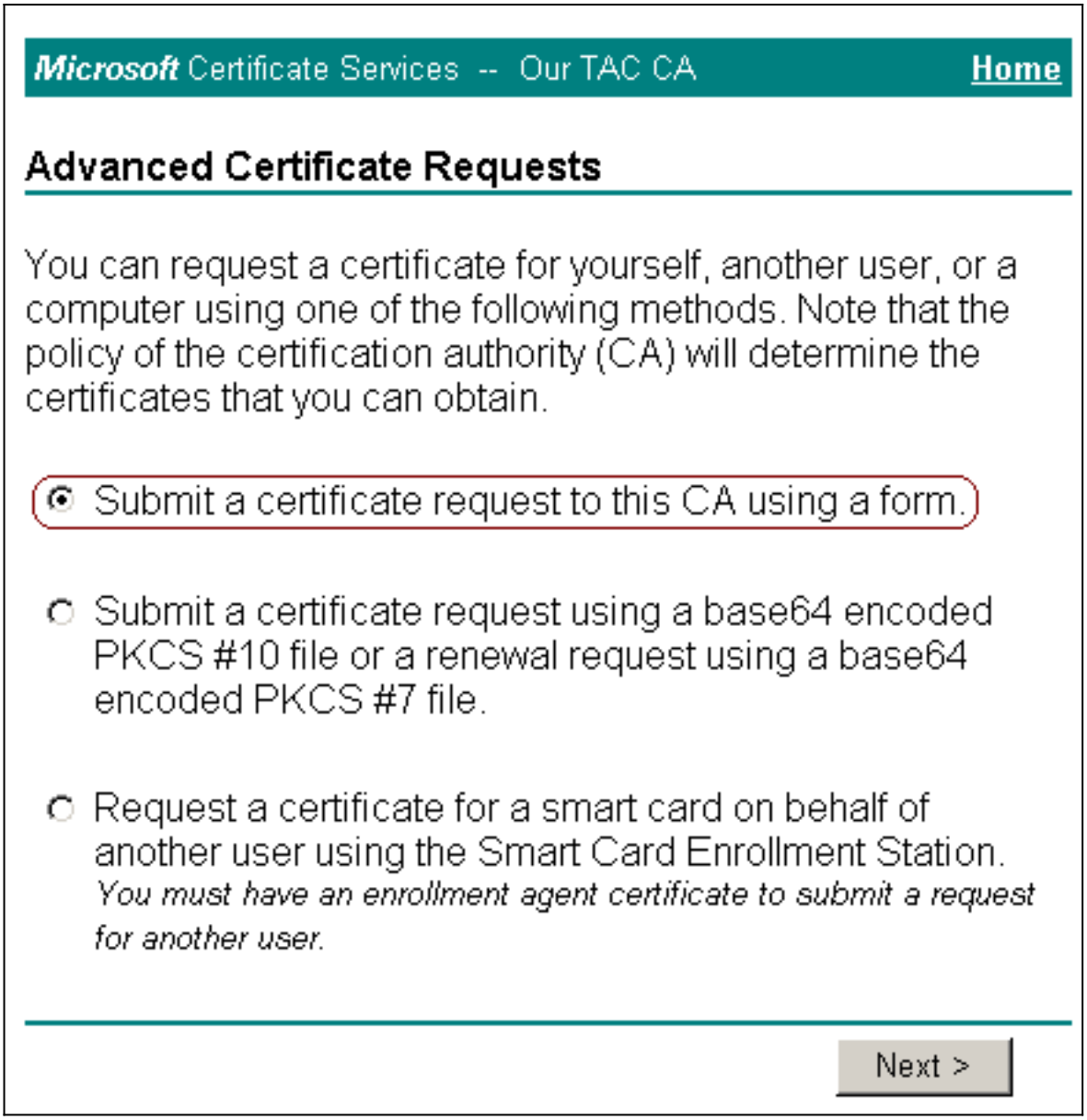
3. Seleccione la **petición un certificado**, y después haga clic **después**.



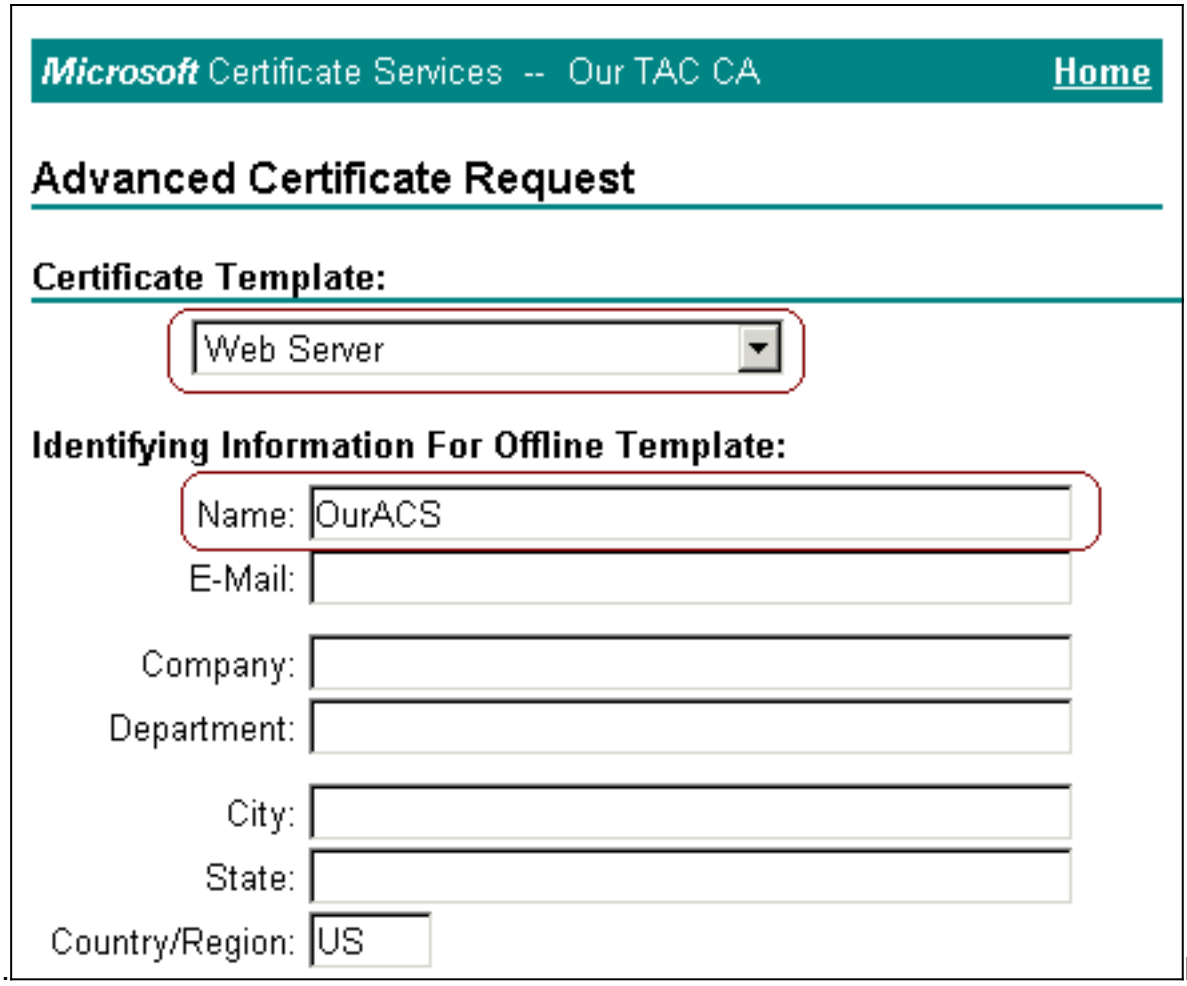
4. Seleccione Advanced request (Petición avanzada) y luego haga clic en Next (Siguiente).



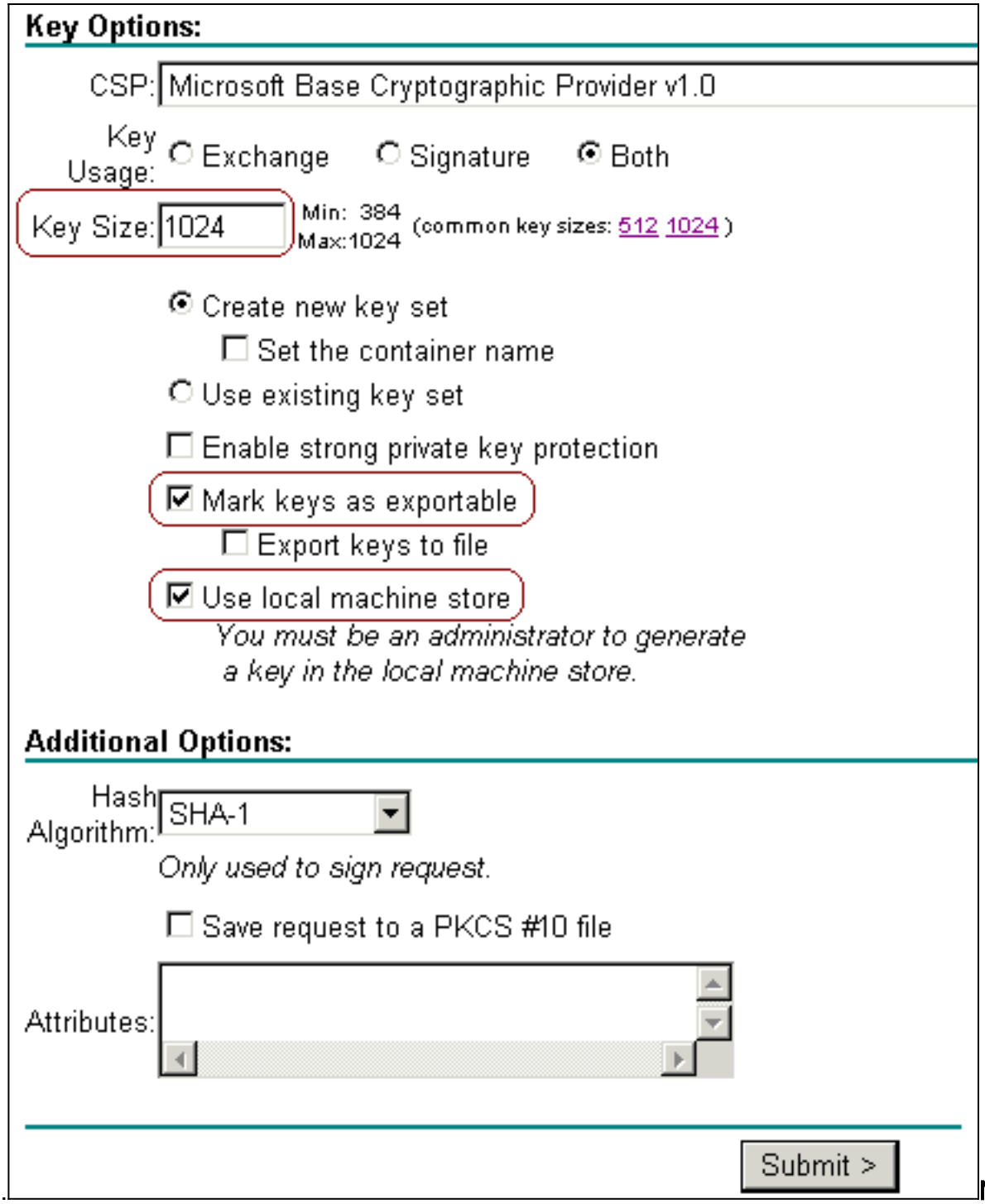
5. Seleccione Submit a certificate request to this CA using a form (Enviar una petición de certificado a esta CA mediante un formulario) y luego haga clic en Next (Siguiente).



6. Configure las opciones del certificado:Seleccione al **servidor Web** como el Certificate Template plantilla de certificado, y ingrese el nombre del servidor



ACS.Ingrese **1024** en el campo del tamaño de clave, y marque las **claves de la marca como exportable** y **utilice las** casillas de verificación del **almacenamiento de máquina local**.Configure las otras opciones que sean necesarias y luego haga clic en Submit

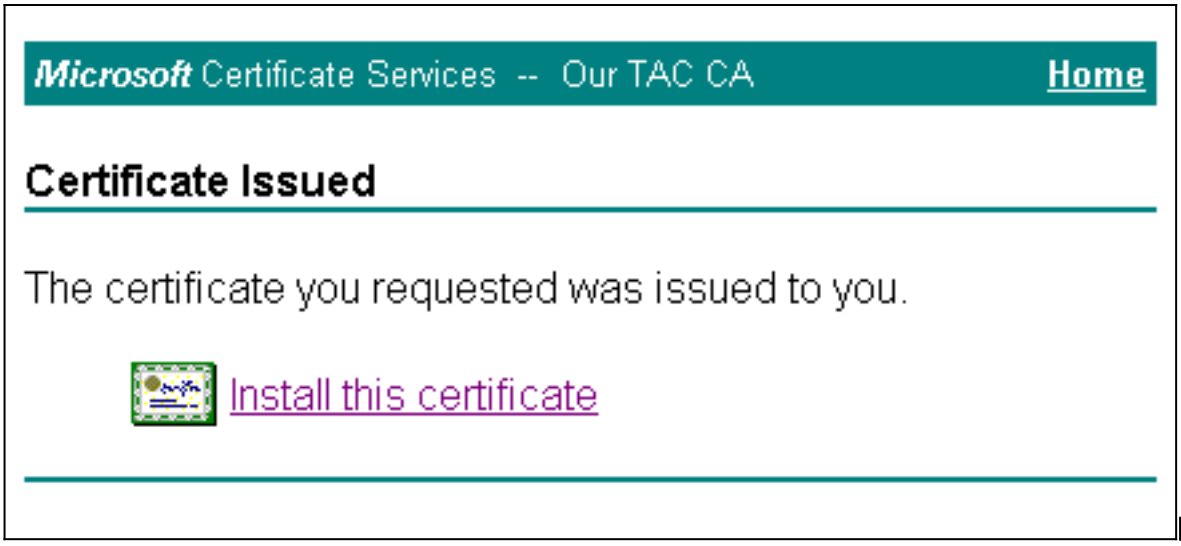


(Enviar).**N**

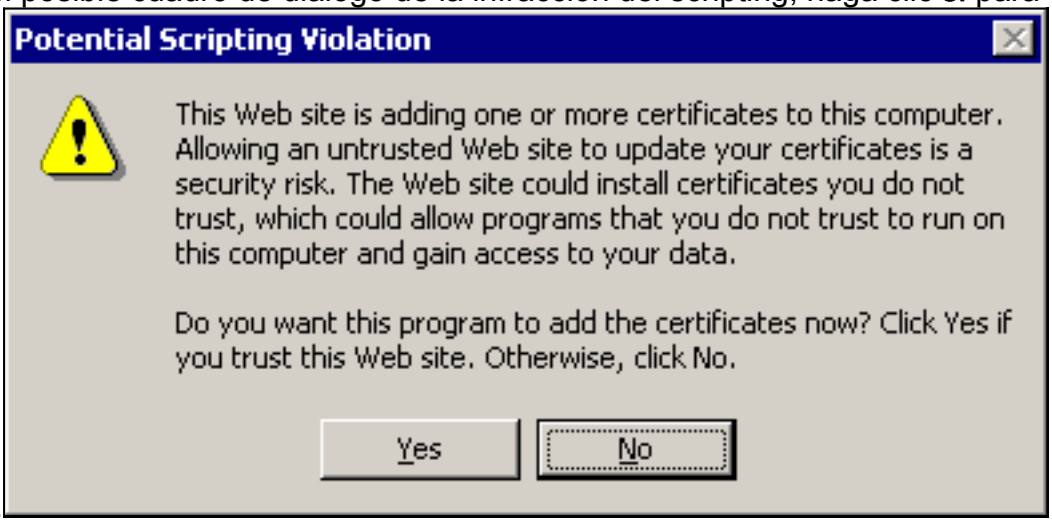
ota: Si aparece el posible cuadro de diálogo de la infracción del scripting, haga clic **sí** para

continuar.

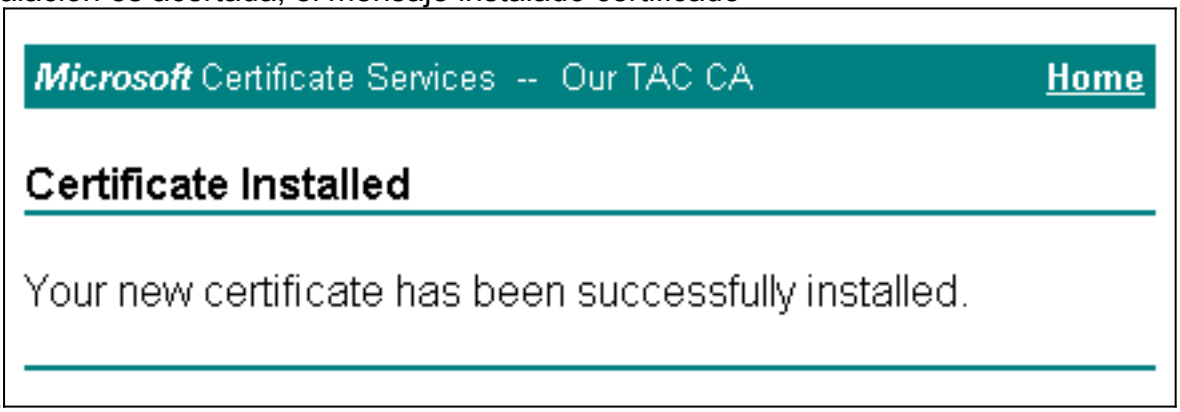
7. Haga clic en Install this certificate (Instalar este certificado).



Nota: Si aparece el posible cuadro de diálogo de la infracción del scripting, haga clic **sí** para continuar.



8. Si la instalación es acertada, el mensaje instalado certificado aparece.



Configure ACS para usar un certificado del almacenamiento

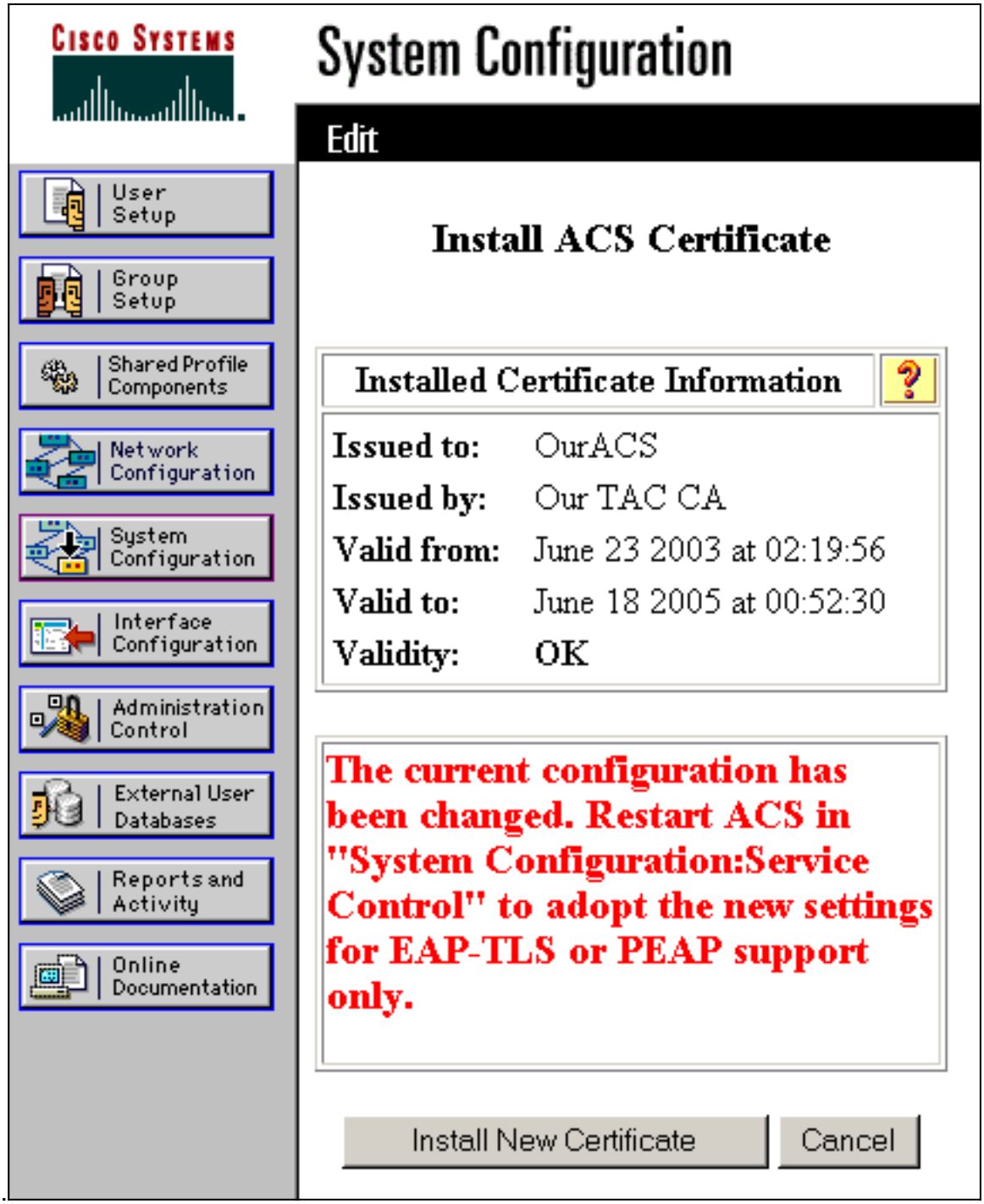
Complete estos pasos para configurar el ACS para utilizar el certificado en el almacenamiento.

1. Abra a un buscador Web, y ingrese **http:// *ACS-ip-address:2002/*** para acceder al servidor ACS.
2. Haga clic en Configuración del sistema, y luego en Instalación de certificado ACS.
3. Haga clic en Install ACS Certificate (Instalar certificado ACS).
4. Haga clic el **certificado del uso del** botón de radio del **almacenamiento**.
5. En el campo del certificado CN, ingrese el nombre del certificado que usted asignó en el

paso 5a de obtener un certificado del ACS Serversection de este documento.

6. Haga clic en Submit

(Enviar).Una vez que la configuración es completa, un mensaje de confirmación aparece que indica que la configuración del servidor ACS se ha cambiado.**Nota:** No es necesario que reinicie el ACS

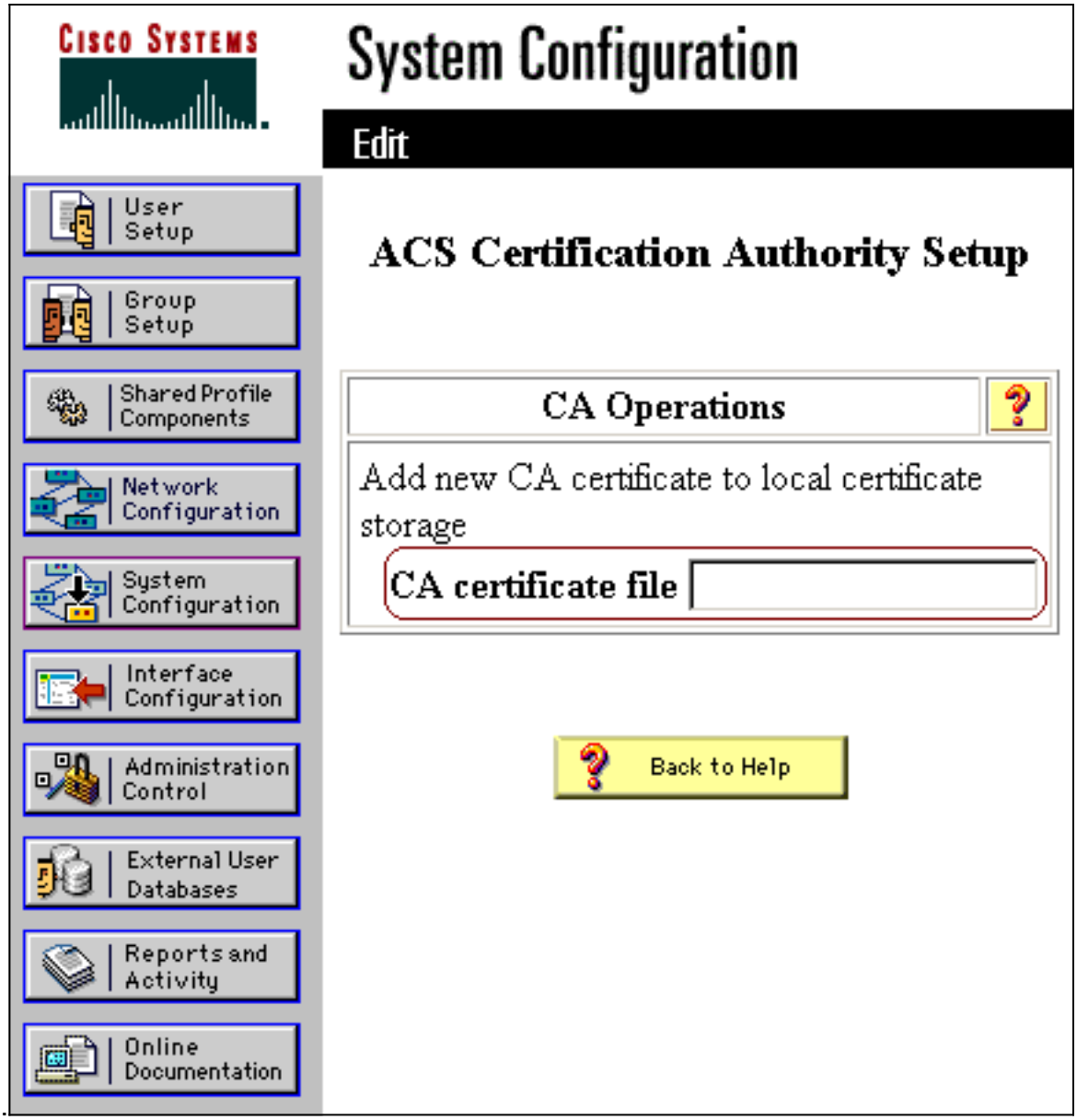


ahora.

Especifique autoridades certificadoras adicionales en las que la ACS debe confiar

El ACS confía en automáticamente CA que publicó su propio certificado. Si los certificados del cliente son publicados por los CA adicionales, usted debe completar estos pasos:

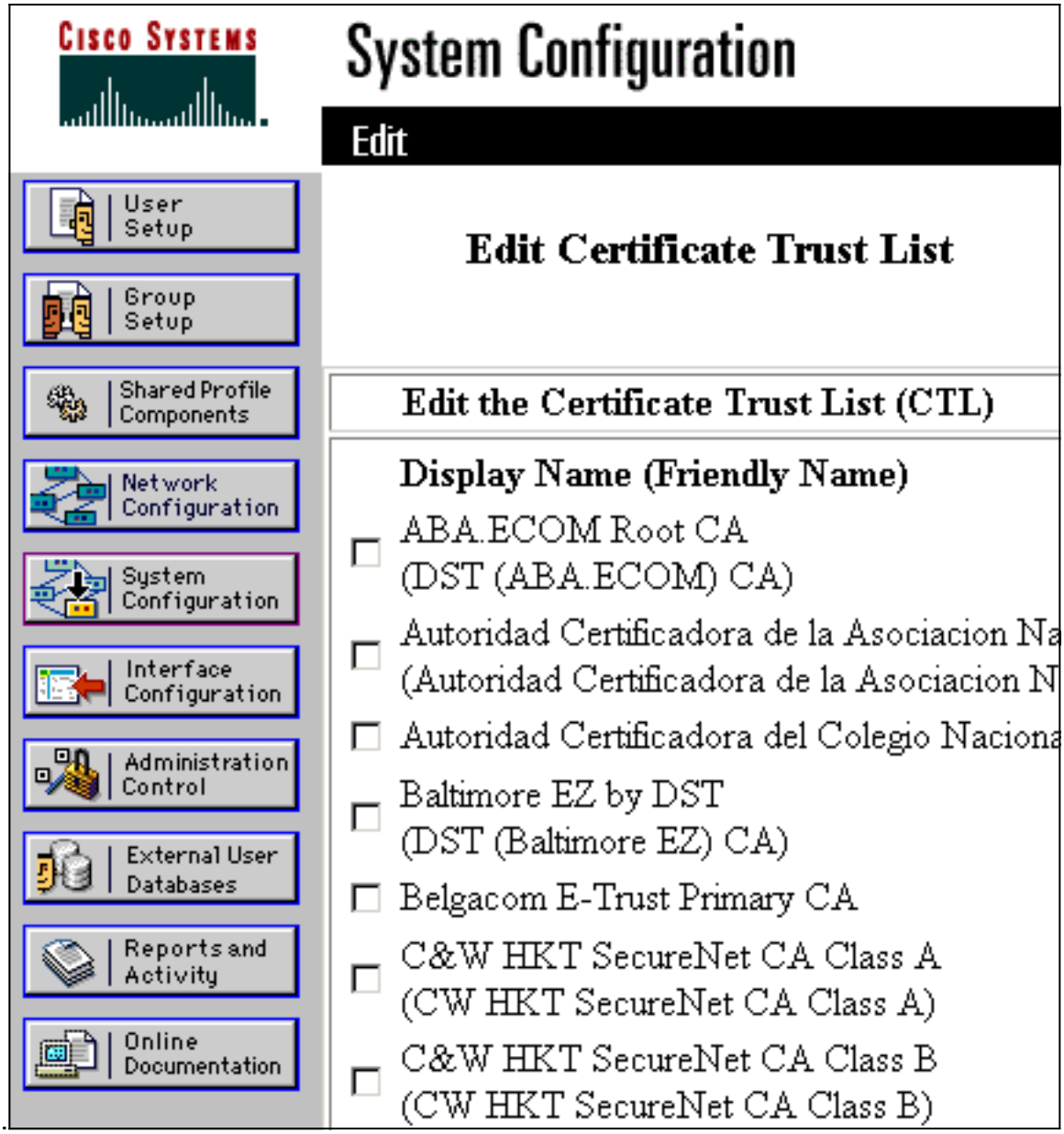
1. Haga clic en Configuración del sistema, y luego en Instalación de certificado ACS.
2. Haga clic en ACS Certificate Authority Setup (Configuración de ACS Certificate Authority) para agregar CA a la lista de certificados confiables.
3. En el campo para el archivo de certificado CA, ingrese la ubicación del archivo y luego haga clic en Submit



(Enviar).

4. Haga clic en Edit Certificate Trust List (Editar lista de confianza del certificado).
5. Marque todos los CA que el ACS debe confiar, y desmarque todos los CA que el ACS no debería confiar.
6. Haga clic en Submit

(Enviar).



Reiniciar el servicio y configurar los parámetros de EAP-TLS en ACS

Complete estos pasos para recomenzar las configuraciones del EAP-TLS del servicio y de la configuración:

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 del EAP-TLS, haga clic la **configuración del sistema**, y después haga clic la **configuración de la autenticación global**.
4. Seleccione Permitir EAP-TLS y luego verifique una o más de las comparaciones de certificado.
5. Haga clic en Submit