Configurar el v3.2 del Cisco Secure ACS for Windows con la autenticación de la máquina PEAP-MS-CHAPv2

Contenido

Introducción

Este documento demuestra cómo configurar el Protocolo de autenticación extensible protegido (PEAP) con la versión 3.2 de Cisco Secure ACS para Windows.

Para más información sobre cómo configurar el acceso de red inalámbrica seguro usando los reguladores del Wireless 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 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**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

PEAP y EAP-TLS crean y usan un túnel de TLS/Secure Socket Layer (SSL) El PEAP utiliza solamente la autenticación del lado del 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 ([AAA] del autenticación, autorización y contabilidad) tienen Certificados y prueban sus identidades el uno al otro.

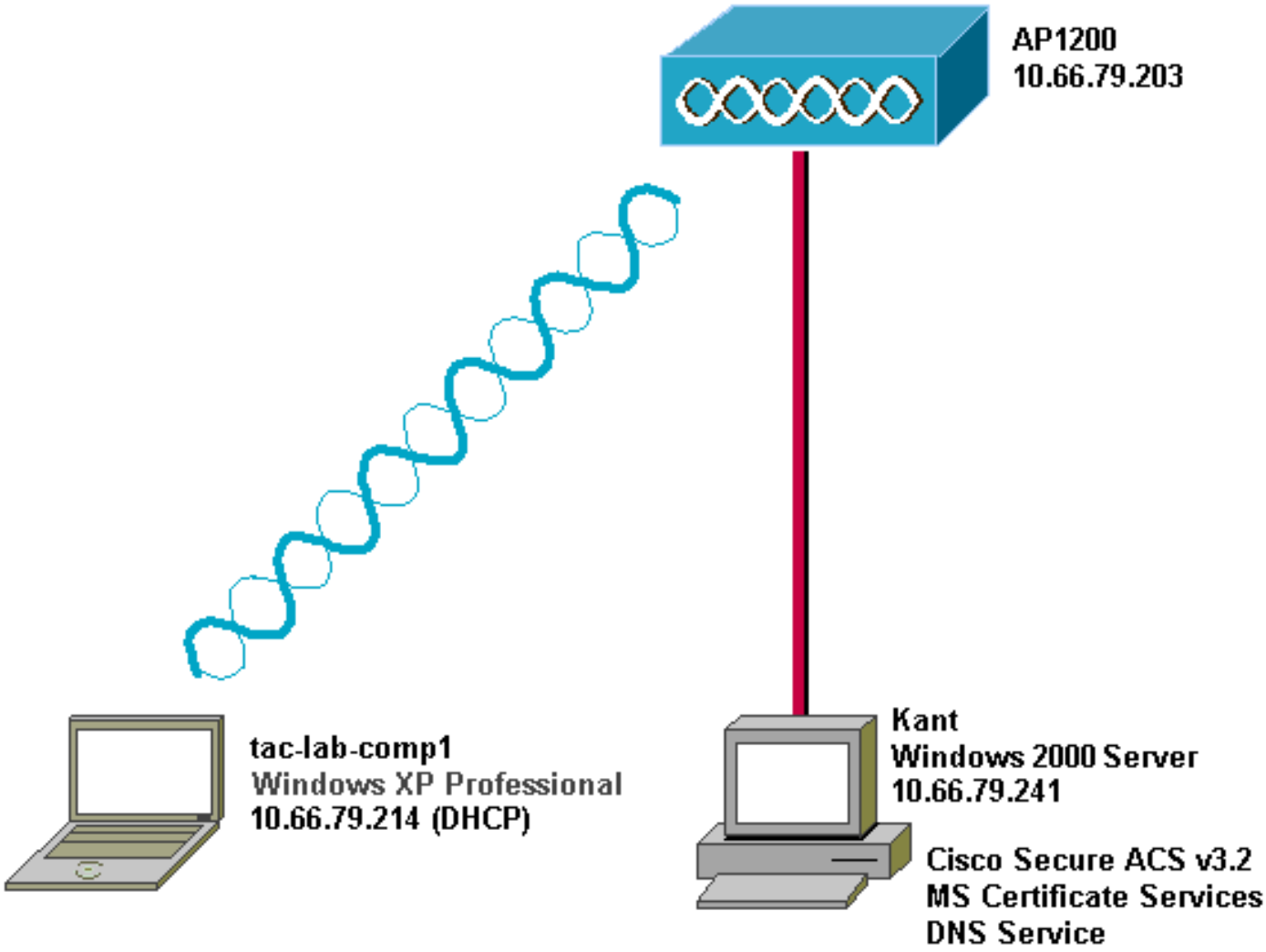
PEAP es conveniente dado que los clientes no requieren certificados. El EAP-TLS es útil para autenticar los dispositivos sin encabezado, porque los Certificados no requieren ninguna interacción del usuario.

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.



V3.2 del Cisco Secure ACS for Windows de la configuración

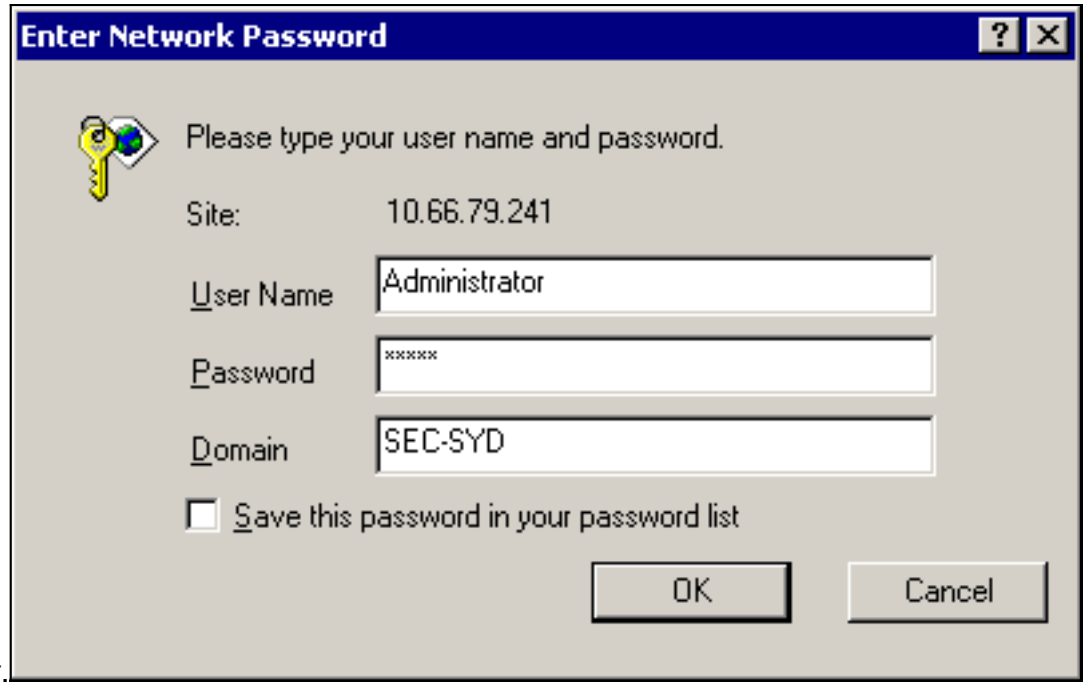
Siga los siguientes pasos para configurar ACS 3.2.

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 los usuarios externos
7. Reiniciar el servicio.

Obtenga un certificado para el servidor ACS

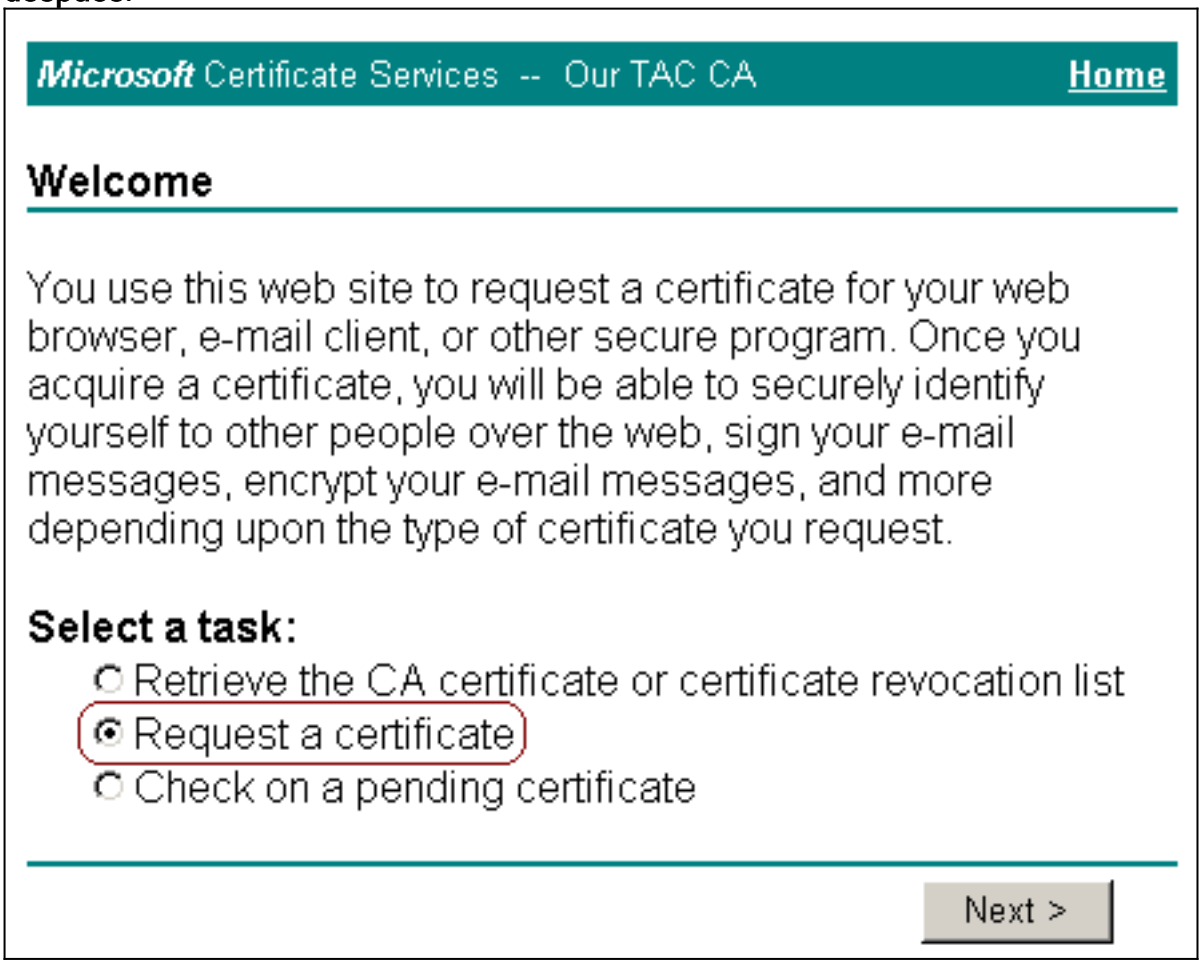
Siga los pasos a continuación para obtener un certificado.

1. En el servidor ACS, abra 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

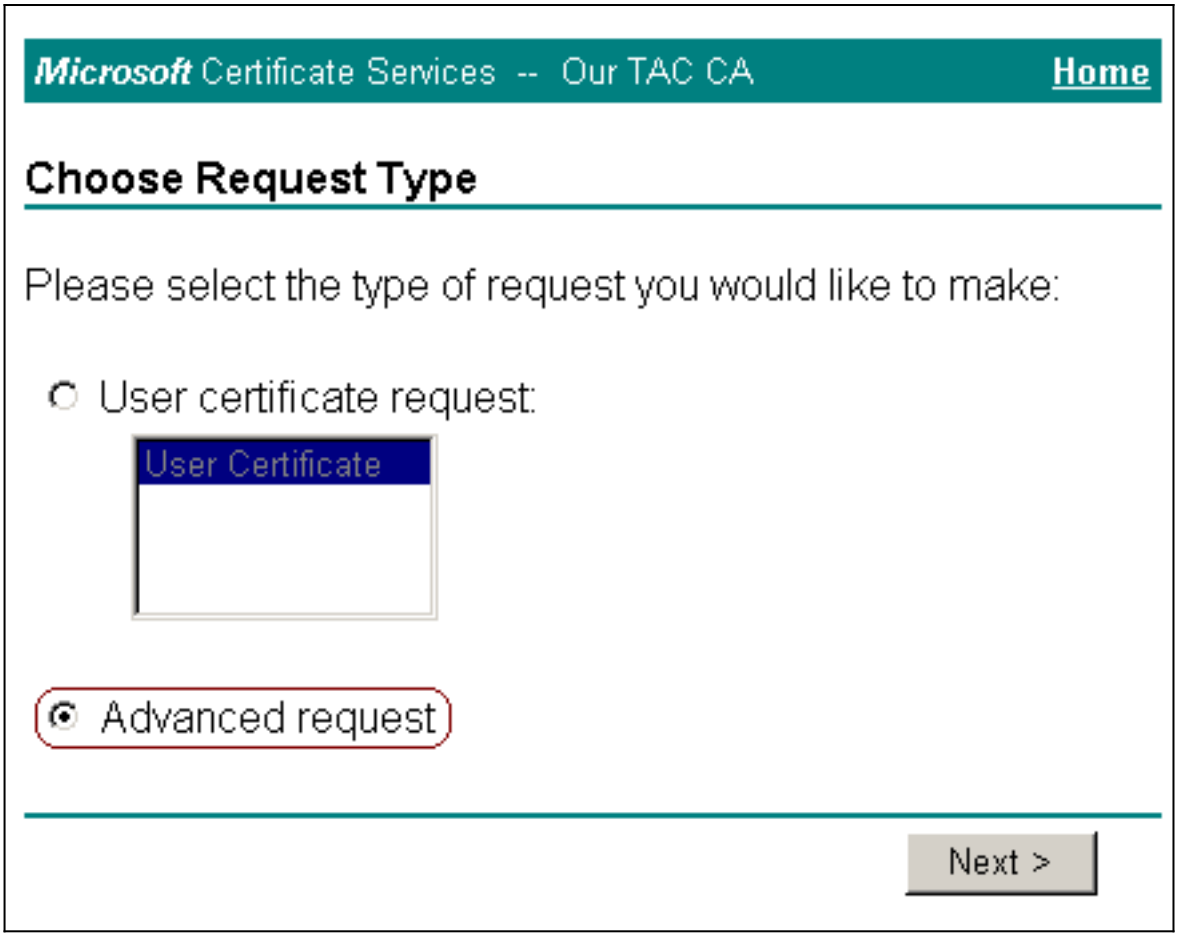


Administrador.

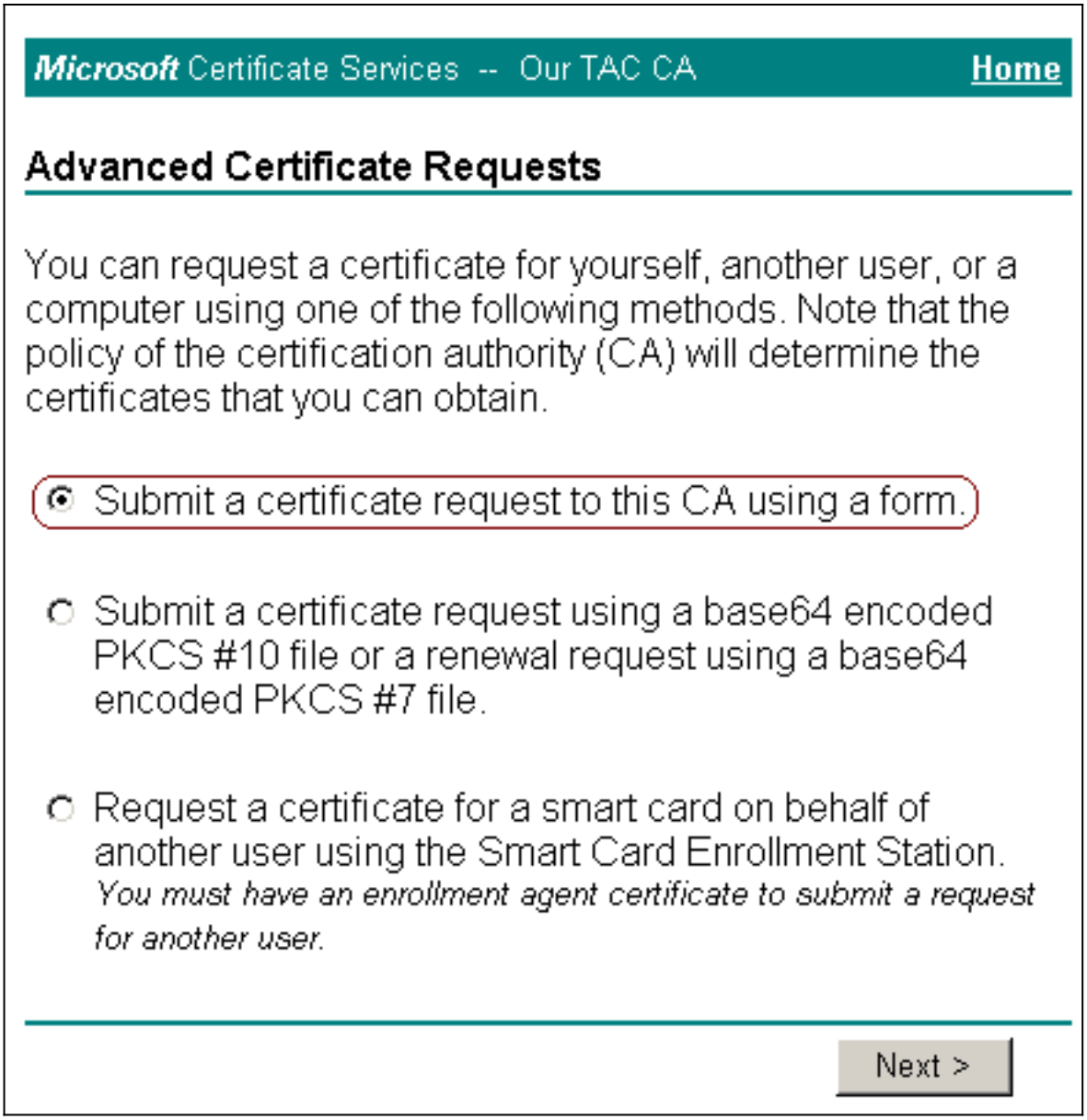
2. Seleccione la **petición un certificado**, y después haga clic **después**.



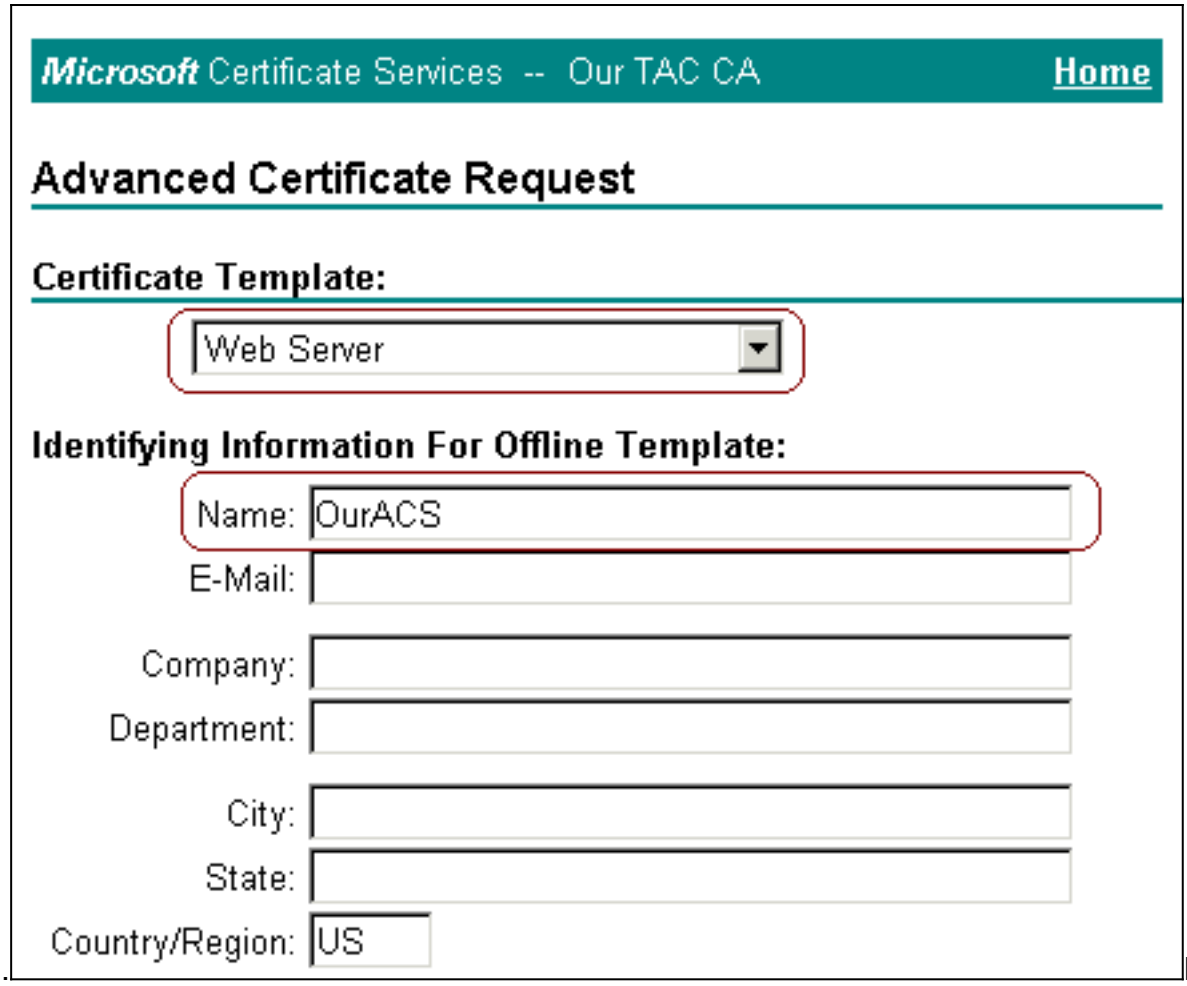
3. Seleccione Advanced request (Petición avanzada) y luego haga clic en Next (Siguiente).



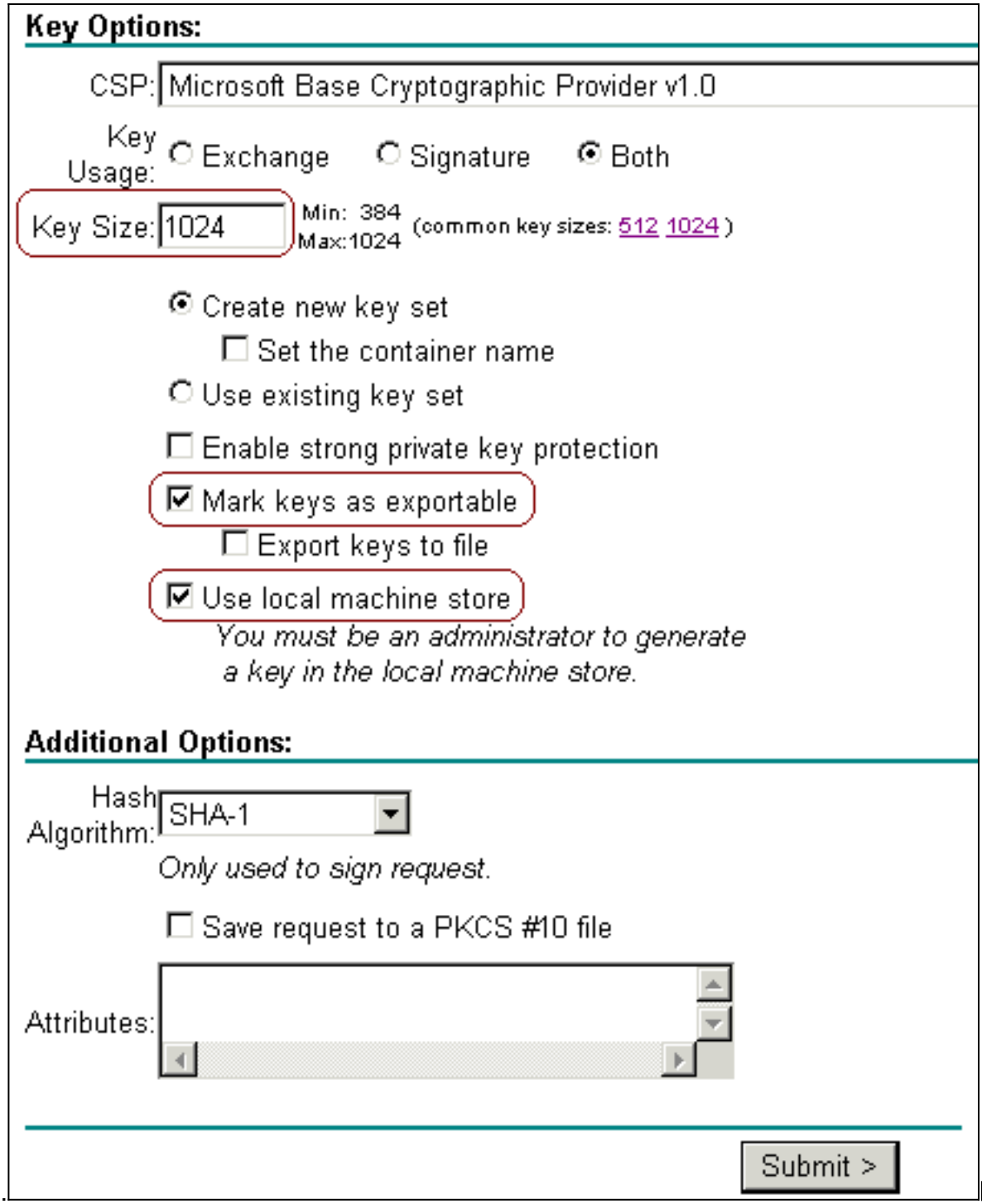
4. Seleccione Submit a certificate request to this CA using a form (Enviar una petición de certificado a esta CA mediante un formulario) y luego haga clic en Next (Siguiente).



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



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

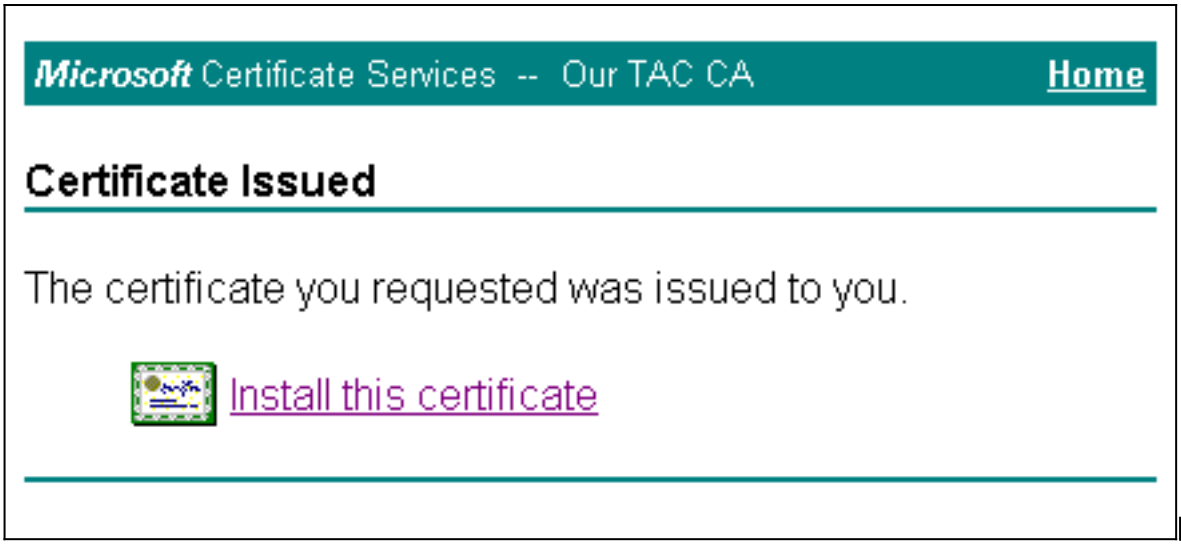


(Enviar).

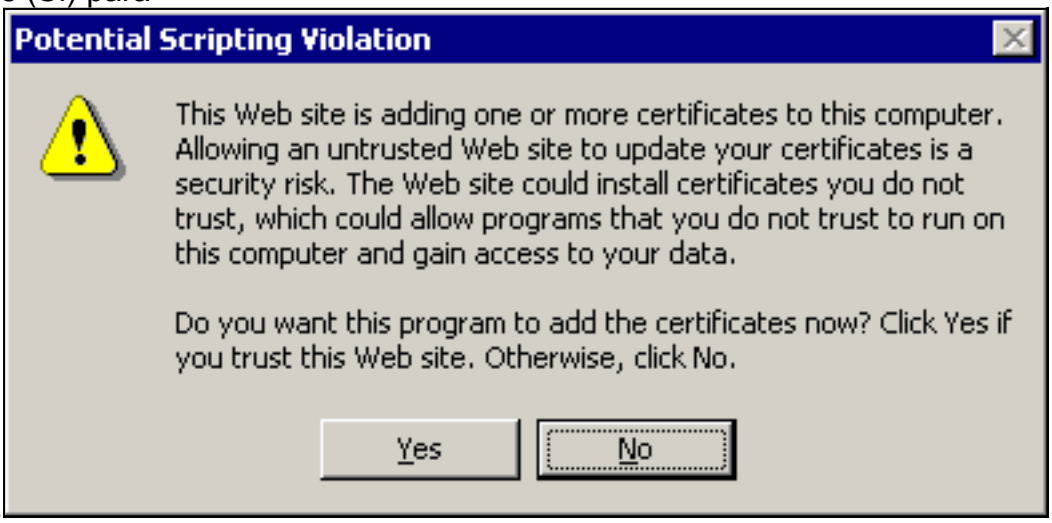
Nota: Si se abre una ventana de advertencia acerca de la falta de cumplimiento de una secuencia de comandos (depende de la configuración de privacidad/seguridad de su navegador), haga clic en Yes (Sí) para

continuar.

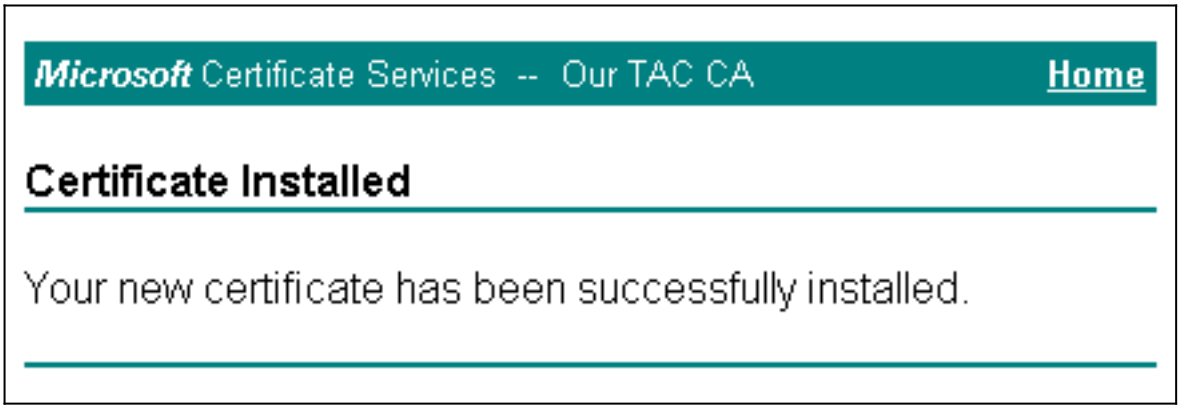
6. Haga clic en Install this certificate (Instalar este certificado).



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

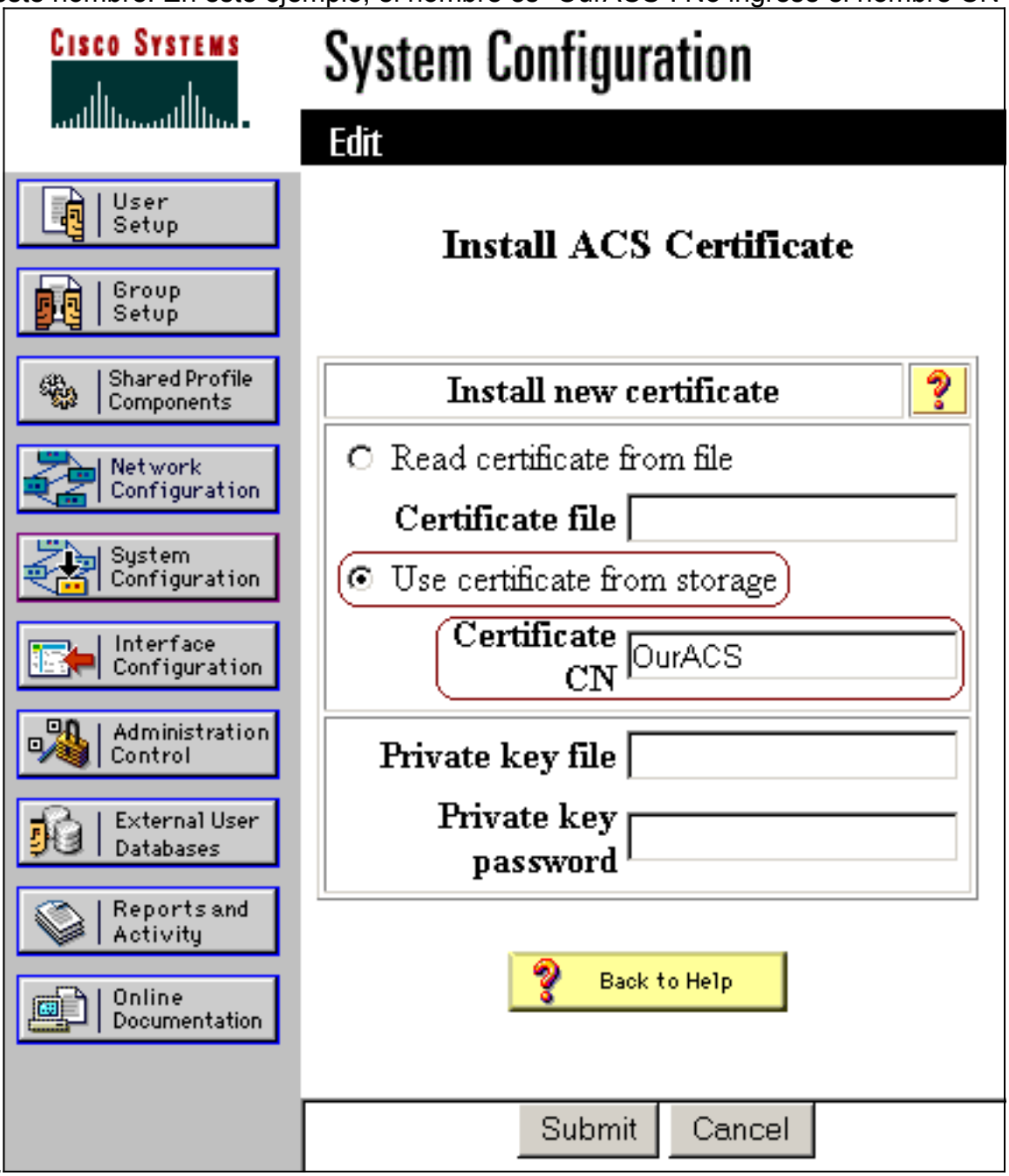


Configure ACS para usar un certificado del almacenamiento

Siga estos pasos para configurar ACS a fin de utilizar el certificado en almacenamiento.

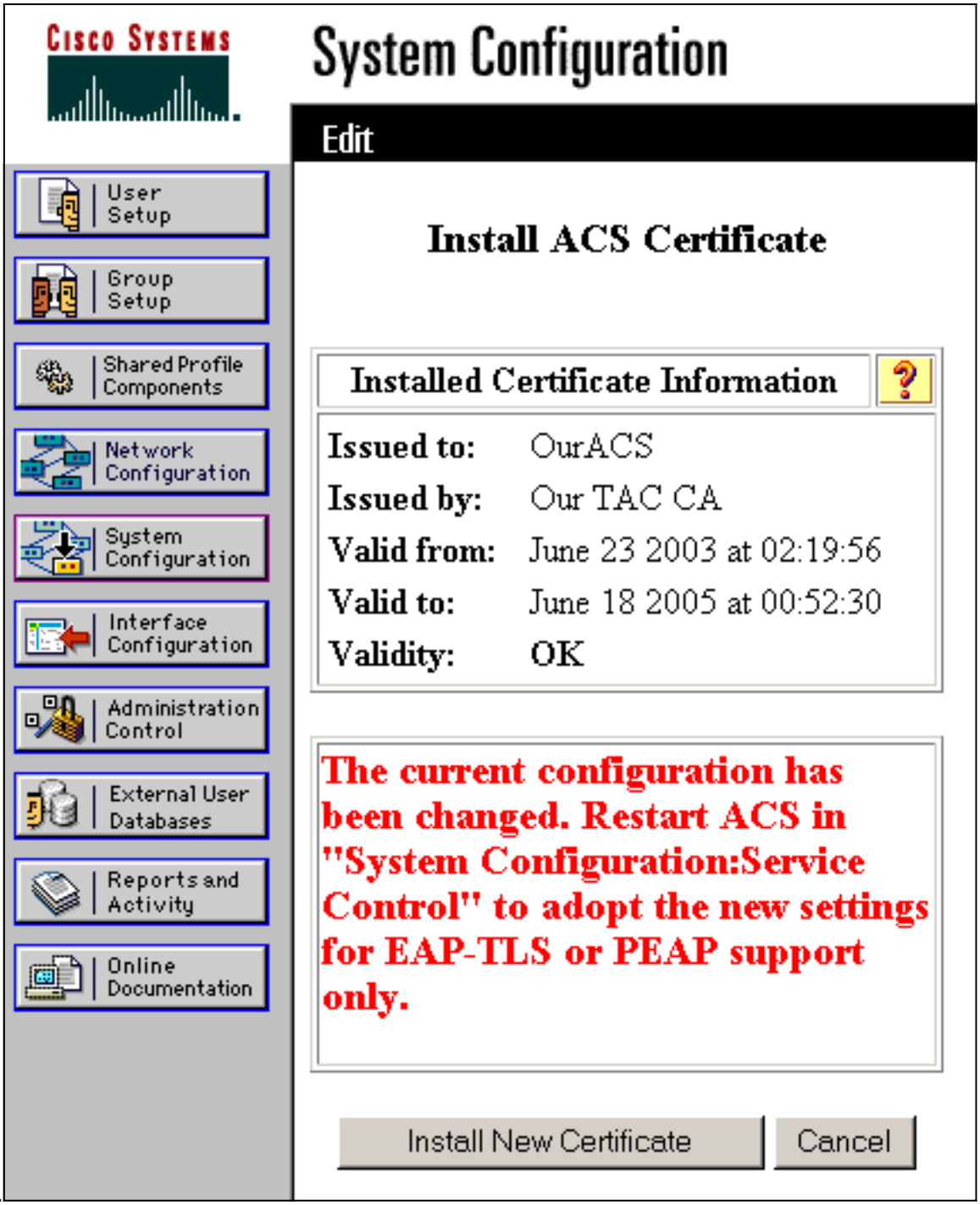
1. Abra un explorador de Web e ingrese http://ACS-ip-address:2002/ en la barra de direcciones para buscar el servidor ACS. Haga clic en Configuración del sistema, y luego en Instalación de certificado ACS.
2. Haga clic en Install ACS Certificate (Instalar certificado ACS).

3. Seleccione Use Certificate from storage (Usar certificado desde almacenamiento). En el campo del certificado CN, 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 coincidir con el nombre que usted escribió en el campo Name (Nombre) durante la solicitud avanzada de certificado. Es el nombre CN en el campo Subject del certificado de servidor; usted puede editar el certificado de servidor para marcar para saber si hay este nombre. En este ejemplo, el nombre es “OurACS”. No ingrese el nombre CN del 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

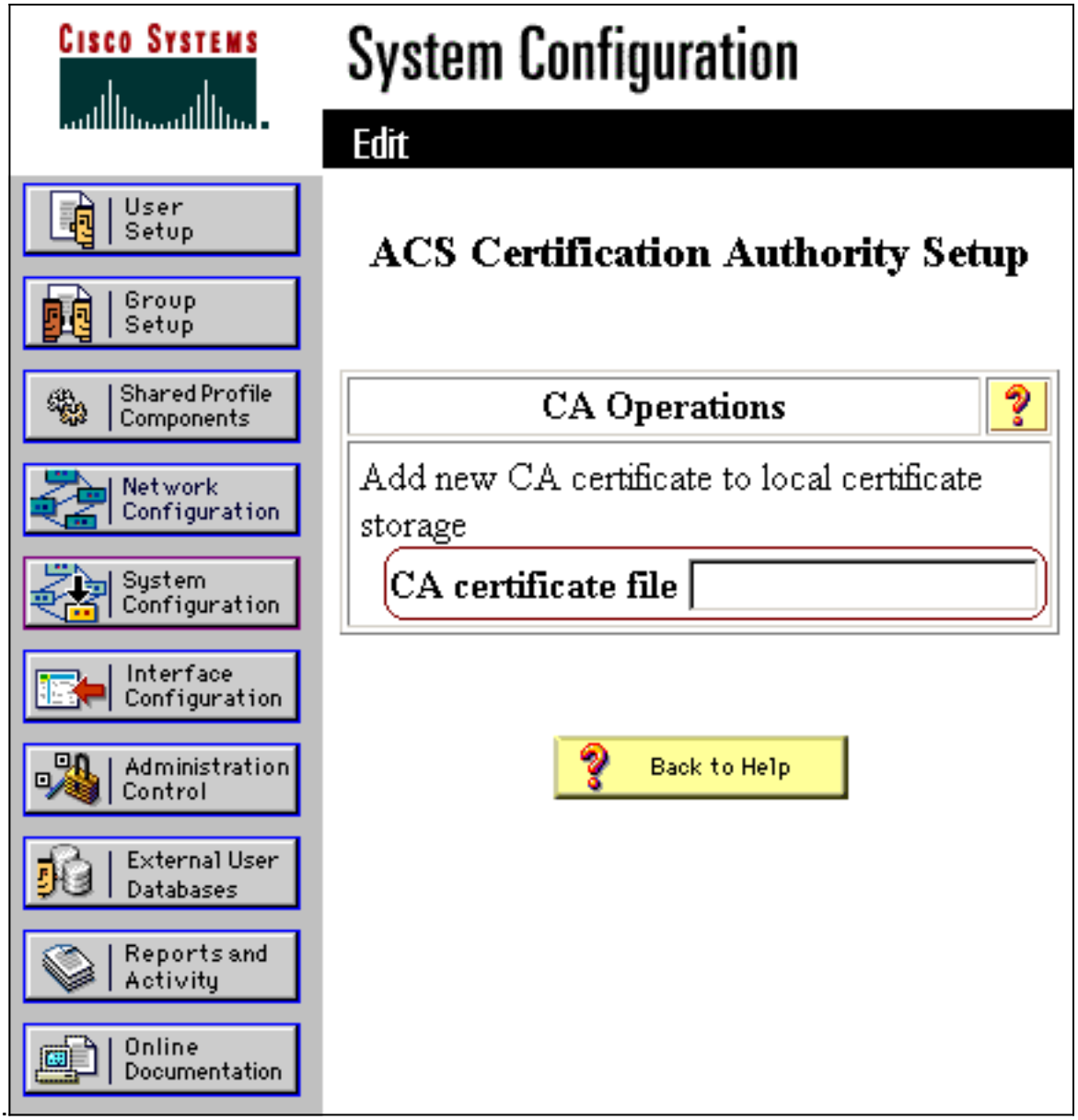
ACS ahora.



Especifique autoridades certificadoras adicionales en las que la ACS debe confiar

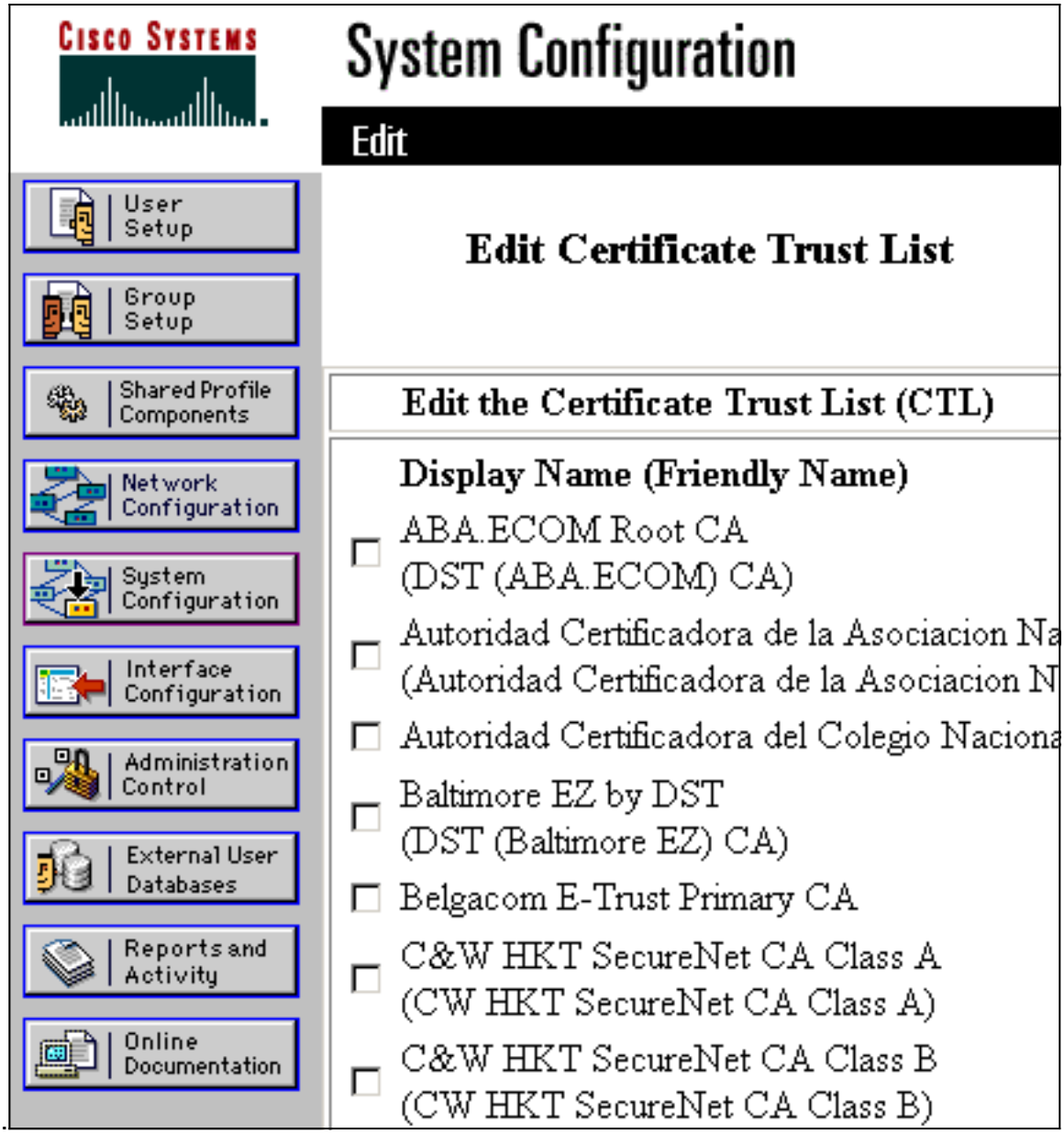
El ACS confiará automáticamente en la Autoridad de certificación que emitió su propio certificado. Si los certificados del cliente están emitidos por Autoridades de certificación, deberá realizar los siguiente pasos:

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. En el campo para el archivo de certificado CA, ingrese la ubicación del archivo y luego haga clic en Submit



(Enviar).

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



(Enviar).

Reinicie el servicio y configure PEAP en el ACS

Siga los siguientes pasos para recomenzar las configuraciones del servicio y de la configuración PEAP.

1. Haga clic en System Configuration (Configuración del sistema), y luego en Service Control (Control del servicio).
2. Haga clic en Restart (Reiniciar) para reiniciar el servicio.
3. Para configurar los valores de PEAP, haga clic en Configuración del sistema, y luego en Configuración de autenticación global.
4. Verifique las dos configuraciones que aparecen a continuación y deje las demás en el modo predeterminado. Si lo desea, puede especificar otras configuraciones adicionales como Enable Fast Reconnect (permitir reconexión rápida). Cuando haya finalizado, haga clic en Submit (Enviar).**Permitir EAP-MSCHAPv2Permite la autenticación de la versión 2 de MS-CHAPNota:** Para obtener más información acerca de Fast Connect, consulte "Authentication Configuration Options" (Opciones de configuración de la autenticación) en System Configuration (Configuración del sistema): Autenticación y certificados.