Secure ACS para Windows v3.2 com autenticação da máquina do EAP-TLS

Índice

Introdução

Este documento descreve como configurar o protocolo extensible authentication – Transport Layer Security (EAP-TLS) com Cisco Secure Access Control System (ACS) para a versão do Windows 3.2.

Nota: A autenticação da máquina não é apoiada com Certificate Authority (CA) de Novell. O ACS pode usar o EAP-TLS para apoiar a autenticação da máquina ao diretório ativo de Microsoft Windows. O cliente do utilizador final pôde limitar o protocolo para a autenticação de usuário ao mesmo protocolo que é usado para a autenticação da máquina. Isto é, o uso do EAP-TLS para a autenticação da máquina pôde exigir o uso do EAP-TLS para a autenticação de usuário. Para obter mais informações sobre da autenticação da máquina, refira a seção da autenticação da

máquina do *Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1*.

Nota: Quando estabelecer o ACS para autenticar máquinas através do EAP-TLS e do ACS estabelecer-se-&z para a autenticação da máquina, o cliente deve ser configurado para fazer a autenticação da máquina somente. Para mais informação, consulte como permitir a autenticação do computador-somente para uma rede 802.1X-based em Windows Vista, em Windows Server 2008, e em Windows XP Service Pack 3.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Cisco Secure ACS para Windows versão 3.2
- Microsoft Certificate Services (instalado como Enterprise root certificate authority [CA])**Nota:** Para obter mais informações, consulte o Manual passo a passo para configurar uma autoridade de certificação.
- Serviço DNS com Windows 2000 Server com Service Pack 3 e hotfix 323172**Nota:** Se tiver problemas com o servidor CA, instale a correção dinâmica 323172. O cliente do Windows 2000 SP3 exige o hotfix 313664 permitir a autenticação do IEEE 802.1X.
- Cisco Aironet 1200 Series Wireless Access Point 12.01T
- IBM ThinkPad T30 executando Windows XP Professional com Service Pack 1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Material de Suporte

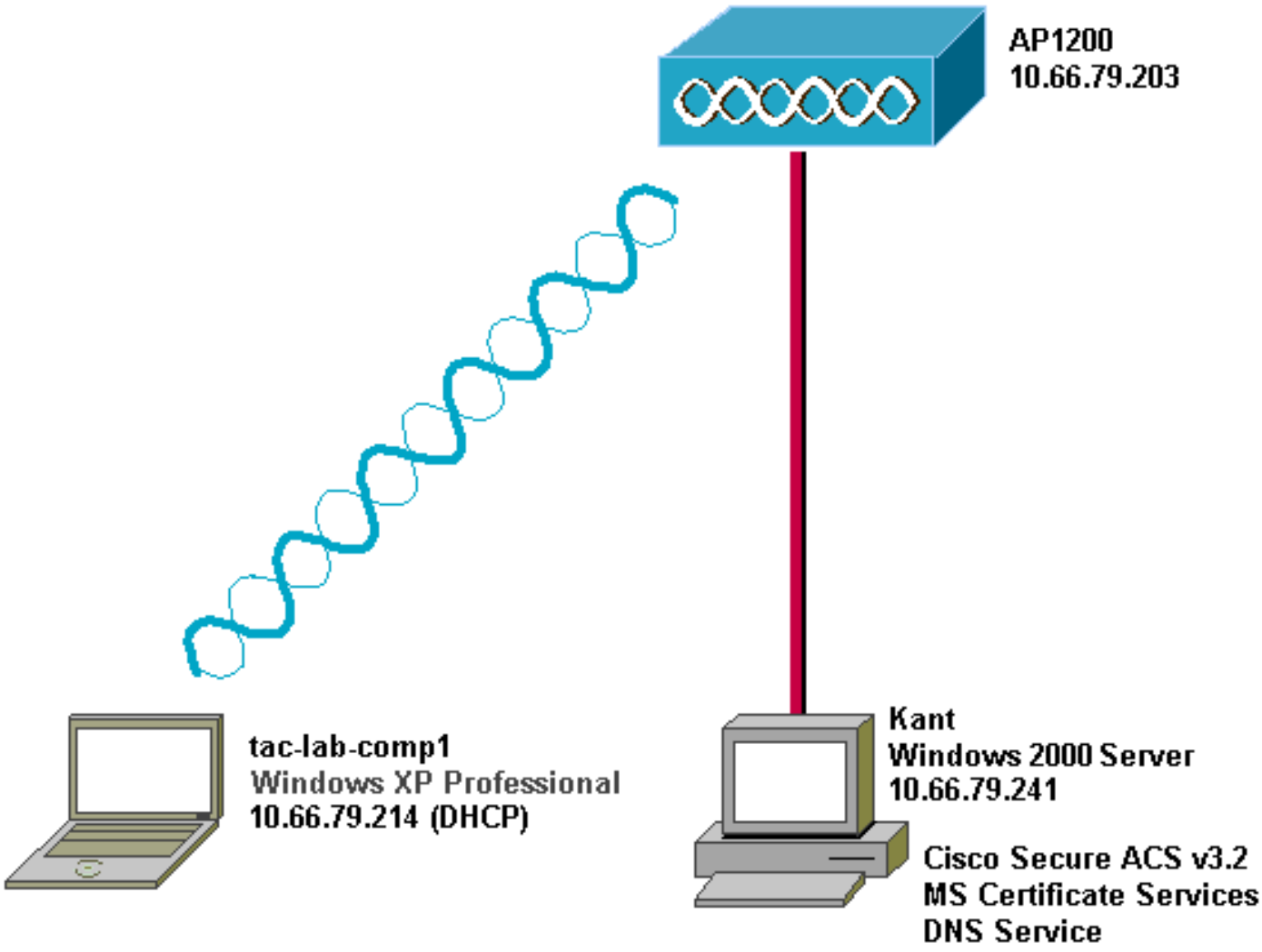
Tanto o EAP-TLS quanto o Protocolo protegido de autenticação extensível (PEAP) criam e utilizam um túnel TLS/Secure Socket Layer (SSL). O EAP-TLS usa a autenticação mútua, na qual tanto o servidor ACS (AAA - autenticação, autorização e relatório) quanto os clientes possuem certificados e comprovam suas identidades uns aos outros. O PEAP, contudo, usa somente a autenticação do lado de servidor; somente o server tem um certificado e prova sua identidade ao cliente.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



Configurando o Cisco Secure ACS for Windows v3.2

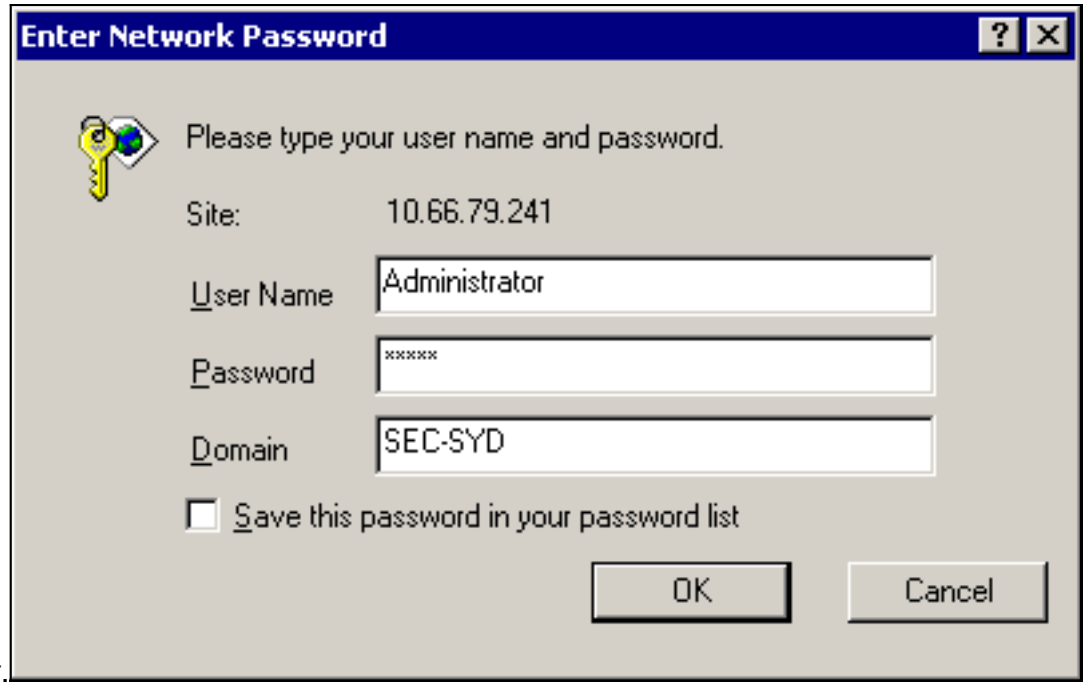
Siga os passos abaixo para configurar o ACS 3.2.

1. Obtenha um certificado para o servidor de ACS.
2. Configure o ACS para utilizar um certificado do armazenamento.
3. Especifique autoridades de certificação adicionais nas quais o ACS deve confiar.
4. Reinicie o serviço e configure as definições PEAP no ACS.
5. Especifique e configure o ponto de acesso como um cliente AAA.
6. Configure os bancos de dados de usuário externo.
7. Reinicie o serviço.

Obtenha um certificado para o servidor ACS

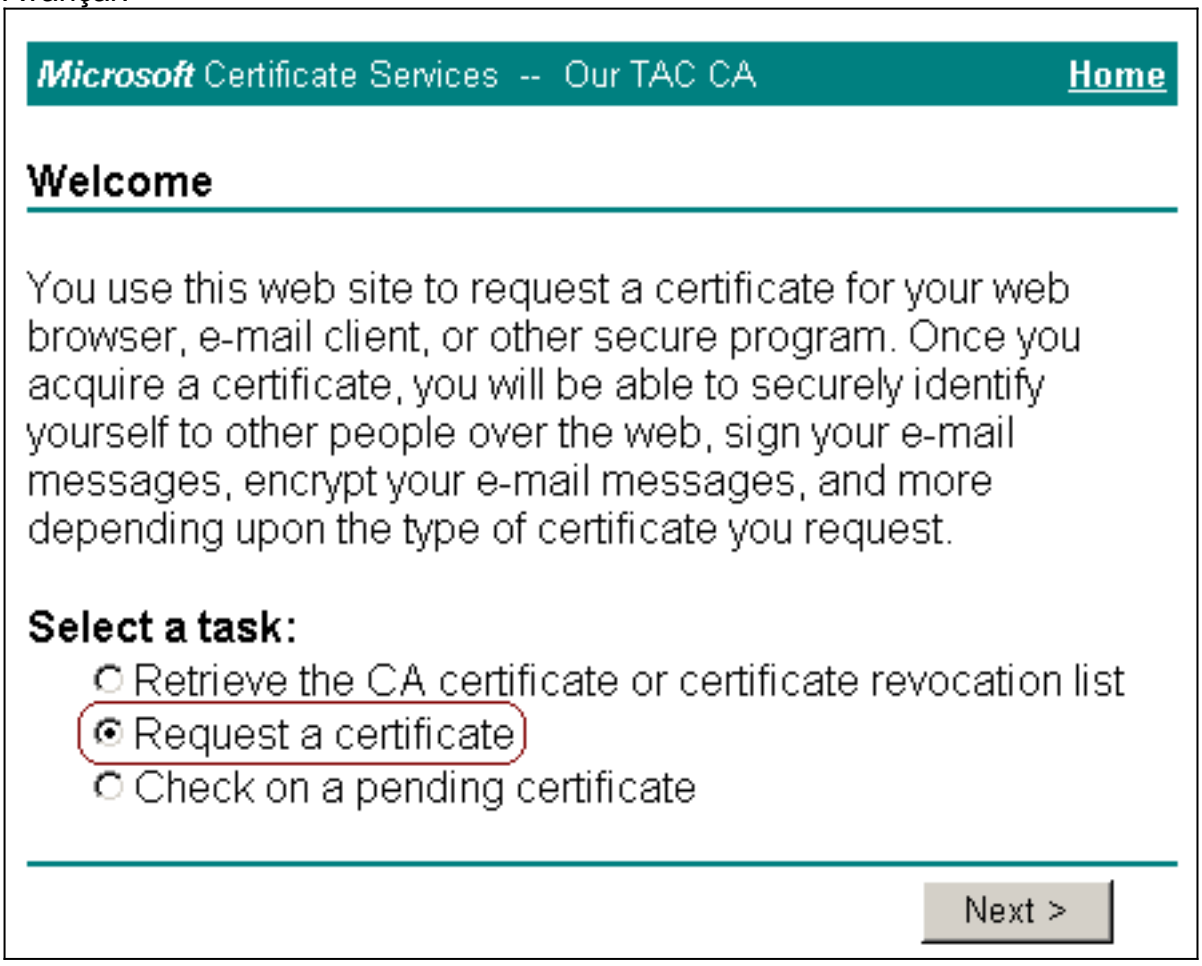
Siga estes passos para obter um certificado.

1. No servidor ACS, abra um navegador da Web, e entre em **http:// CA-ip-address/certsrv** a fim alcançar o server de CA.
2. Efetuar logon no domínio como

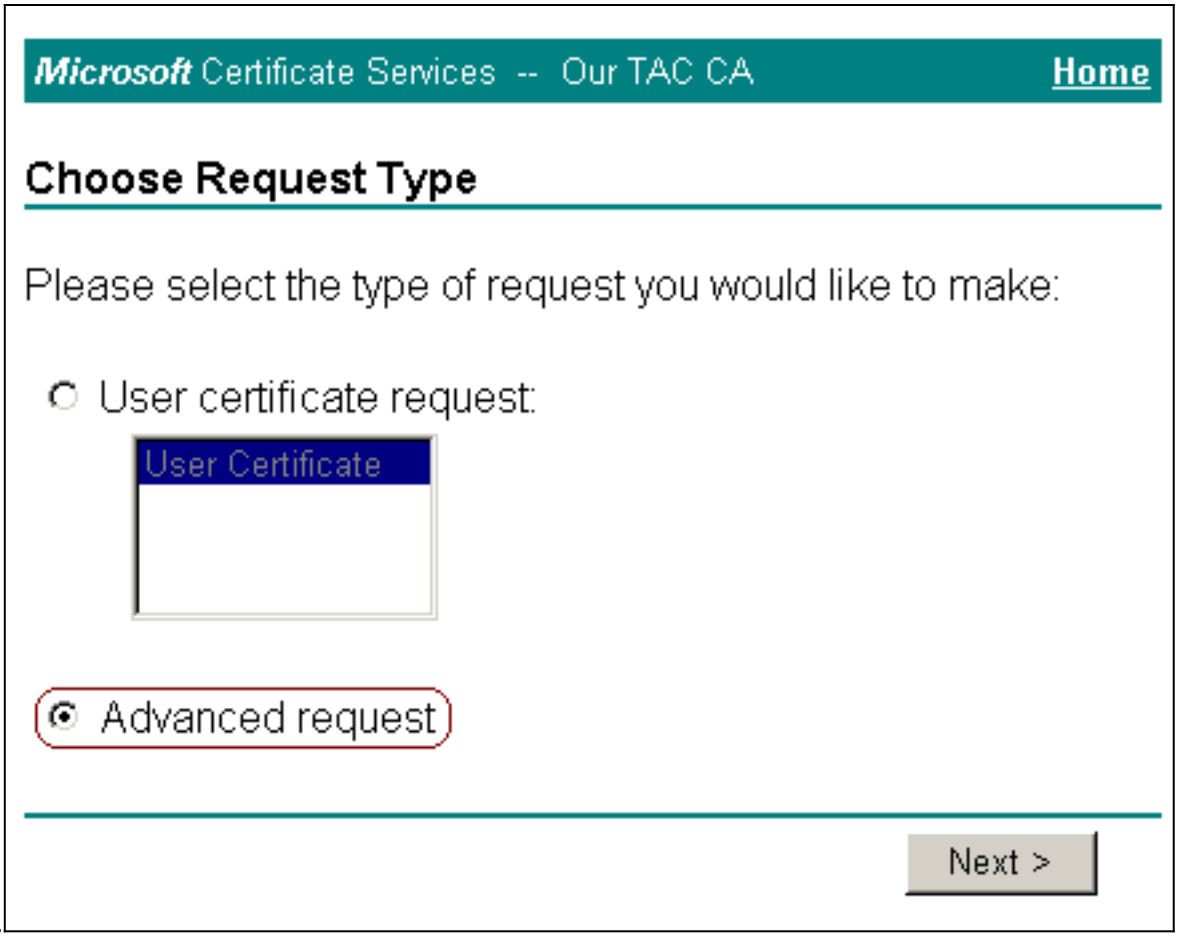


Administrador.

3. Selecione Solicitar um certificado e, em seguida, clique em Avançar.

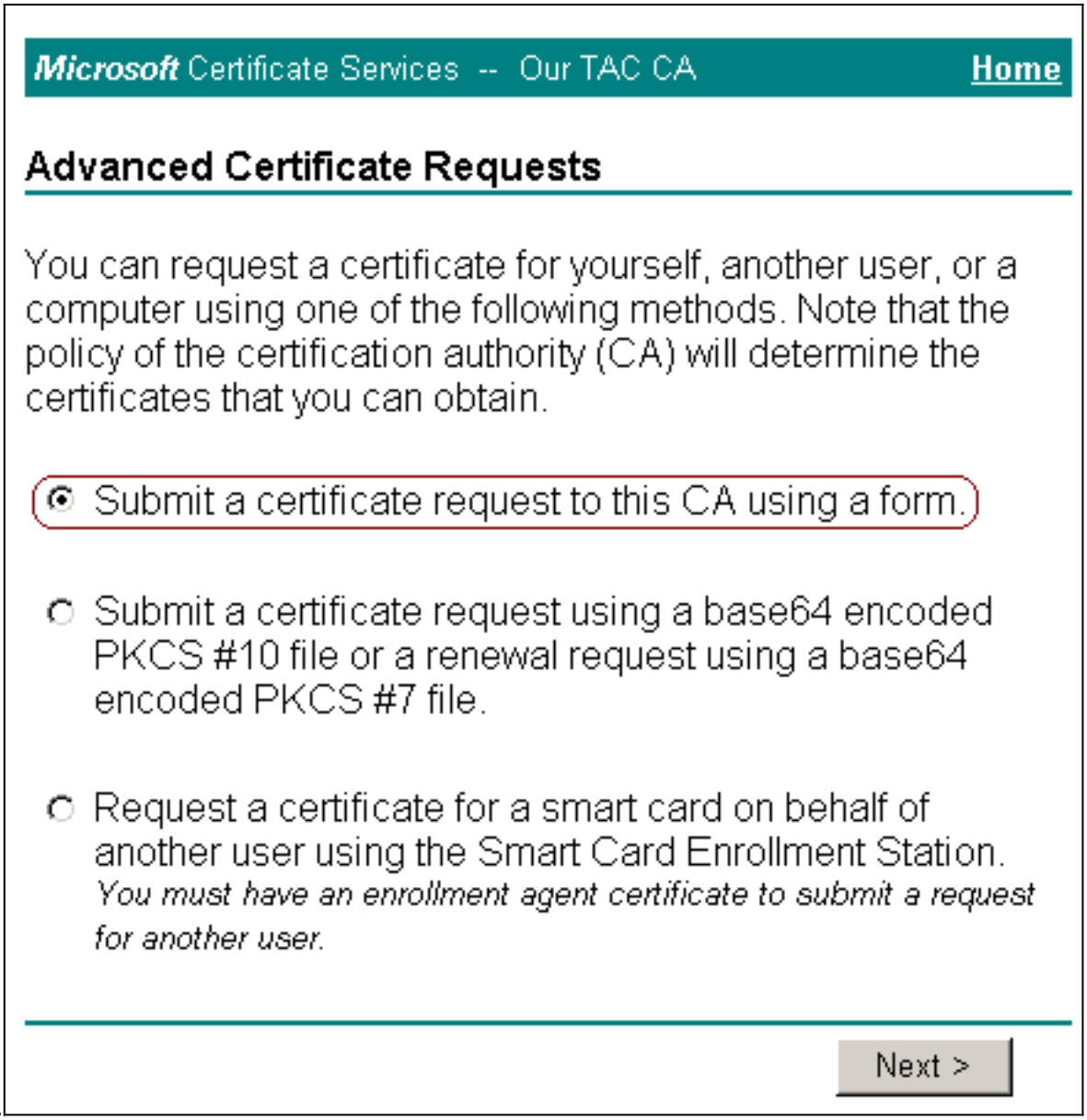


4. Selecione a solicitação Avançado e clique em



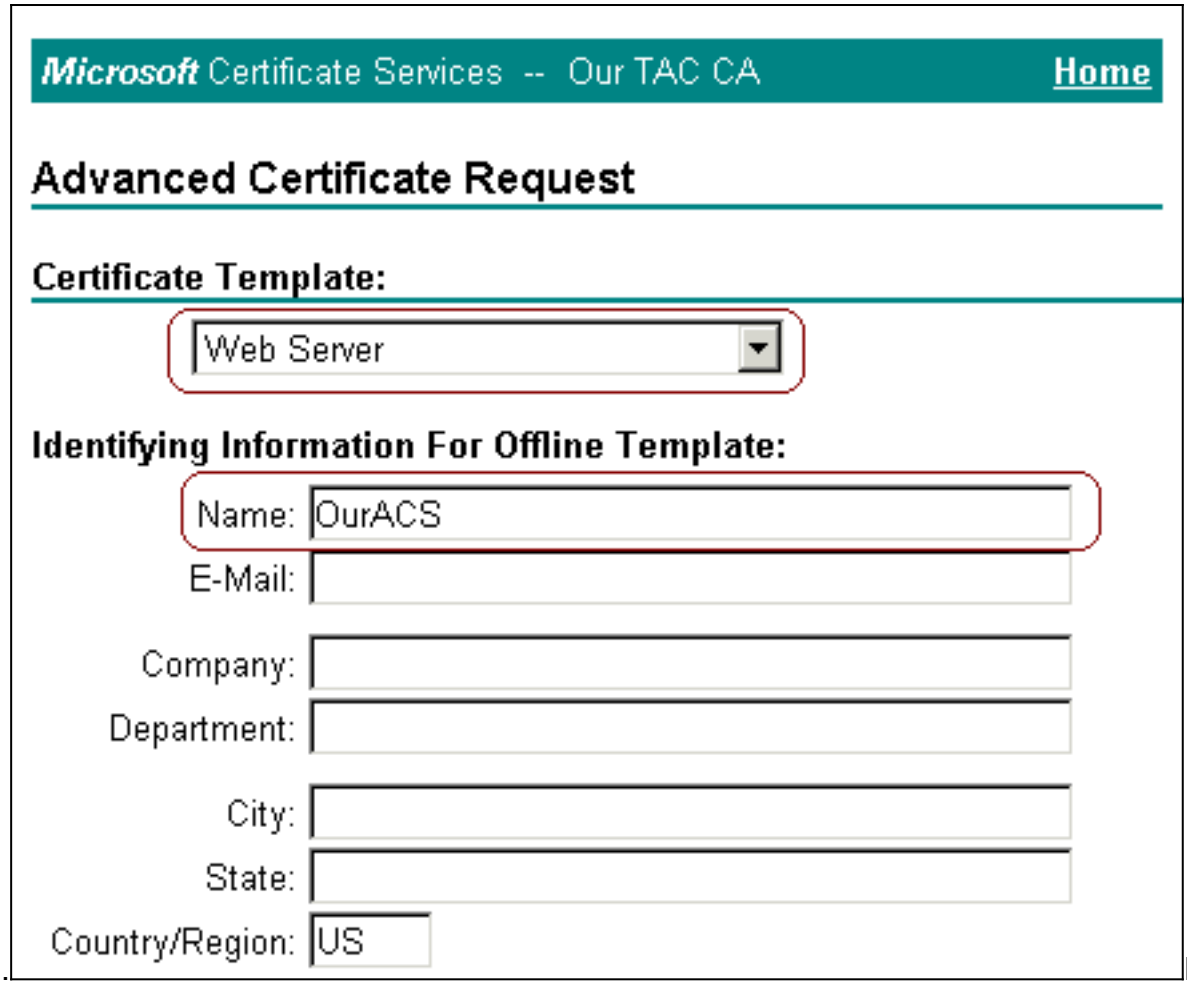
Avançar.

5. Selecione Enviar uma solicitação de certificado para este CA, utilizando um formulário e, em seguida, clique em

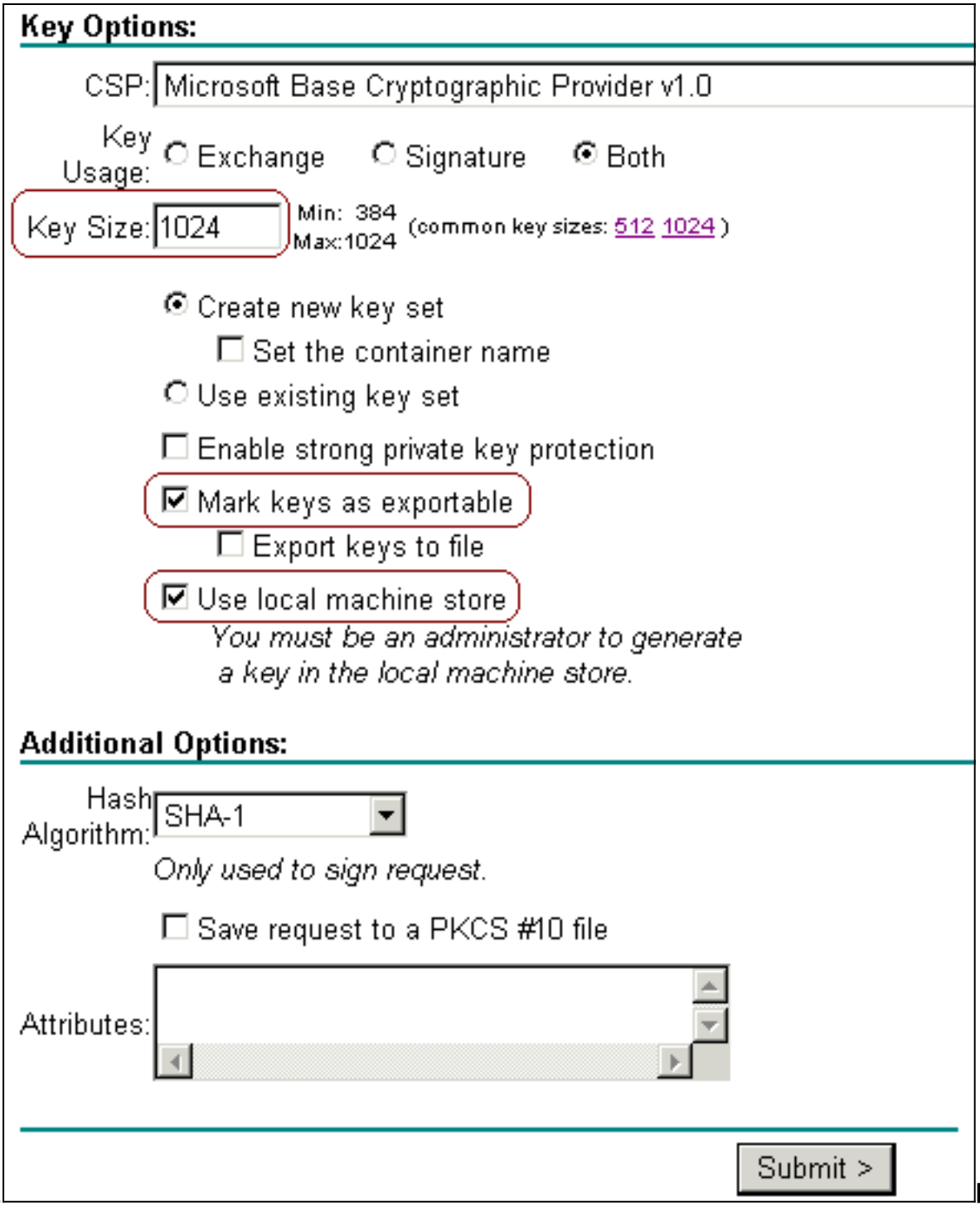


Avançar.

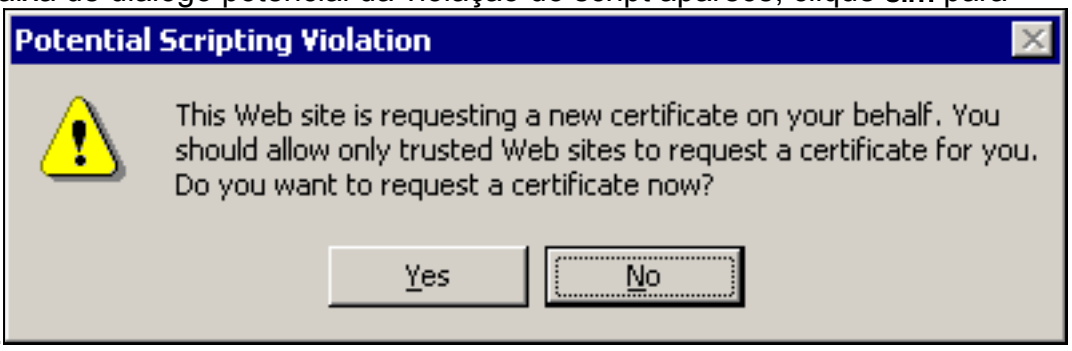
6. Configurar as opções do certificado:Selecione o **servidor de Web** como o molde de certificado, e dê entrada com o nome do servidor



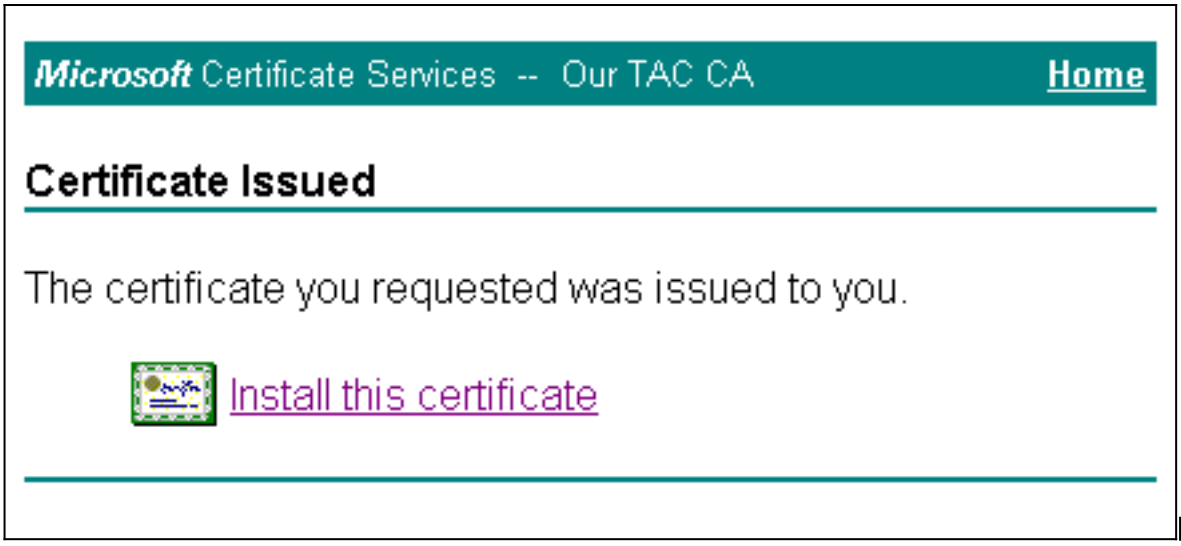
ACS.Incor pore **1024 ao** campo do tamanho chave, e verifique as **chaves de Mark como exportable** e **use** caixas de seleção da **loja de máquina local**.Configure outras opções, conforme necessário e, em seguida, clique em



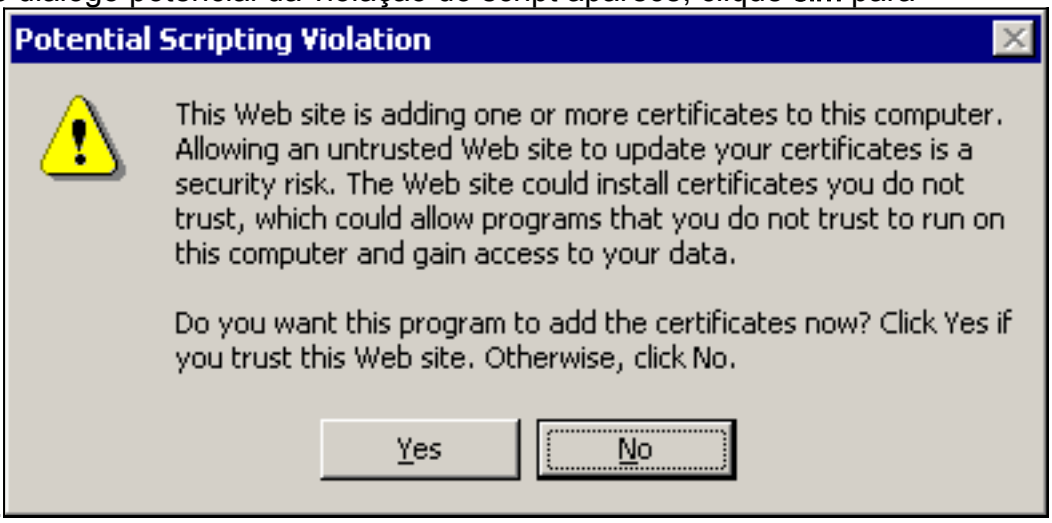
Enviar. **Nota:** Se a caixa de diálogo potencial da violação do script aparece, clique **sim** para continuar.



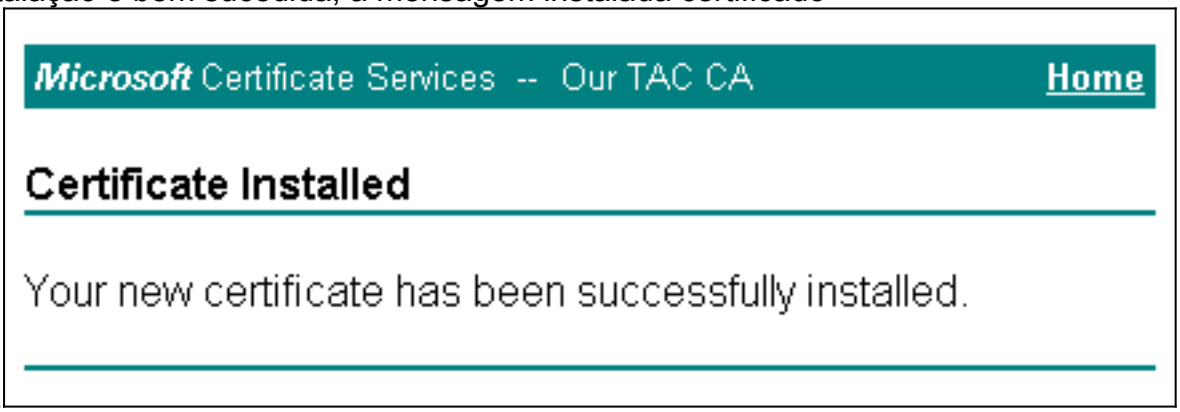
7. Clique em Instalar este certificado.



Nota: Se a caixa de diálogo potencial da violação do script aparece, clique **sim** para continuar.



8. Se a instalação é bem sucedida, a mensagem instalada certificado aparece.



Configurar o ACS para utilizar um certificado do armazenamento

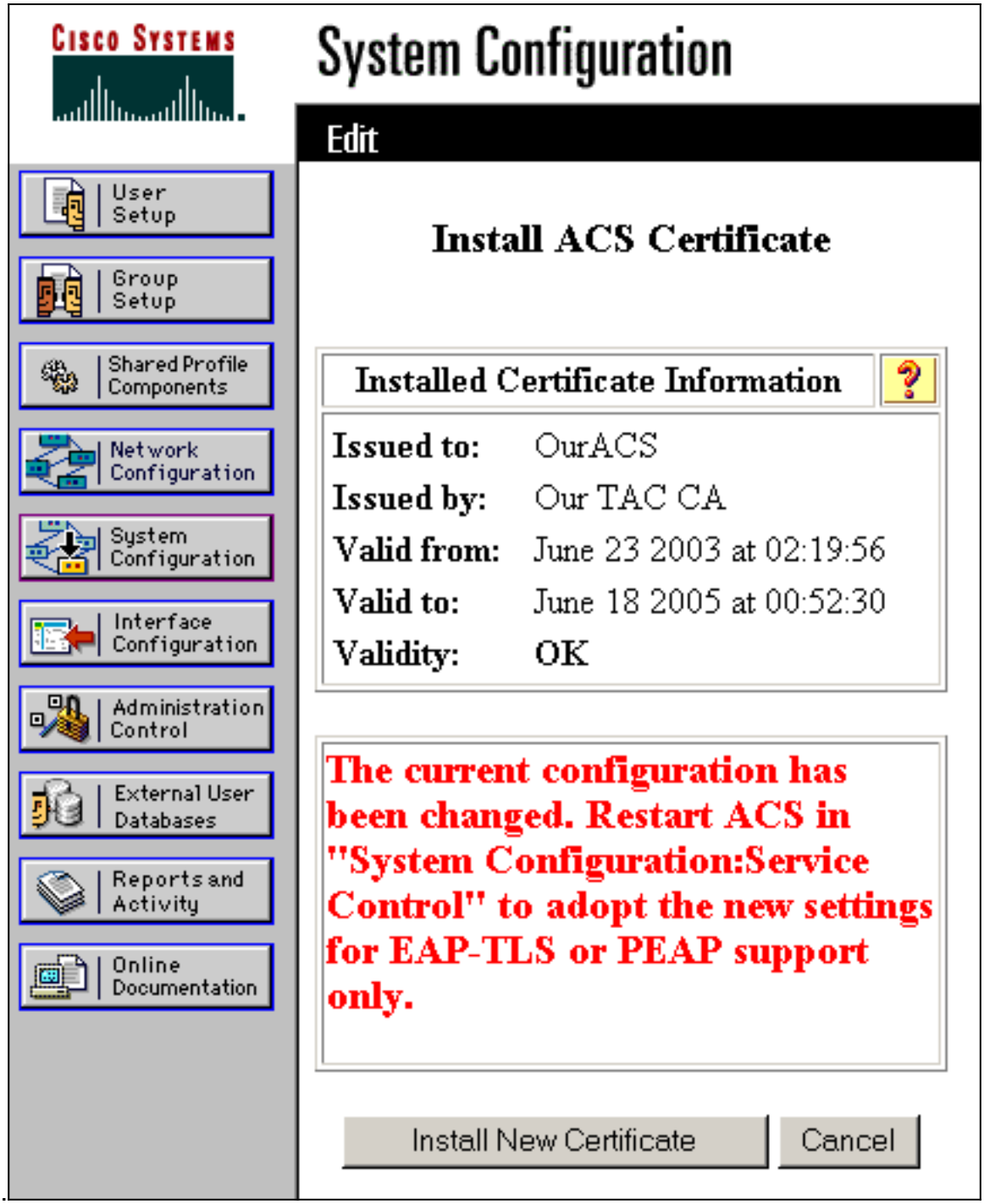
Termine estas etapas a fim configurar o ACS para usar o certificado no armazenamento.

1. Abra um navegador da Web, e entre em **http:// *ACS-ip-address:2002/*** a fim alcançar o servidor ACS.
2. Clique em System Configuration e, em seguida, em ACS Certificate Setup.
3. Clique em Install ACS Certificate (Instalar certificado ACS).
4. Clique o **certificado do uso do** botão de rádio do **armazenamento**.
5. No campo do CN do certificado, dê entrada com o nome do certificado que você atribuiu na

etapa 5a de obter um certificado do ACS Serversection deste documento.

6. Clique em Submit.

Um a vez que a configuração está completa, um mensagem de confirmação aparece que indique que a configuração do servidor ACS esteve mudada.**Nota:** Você não precisa reiniciar o ACS desta

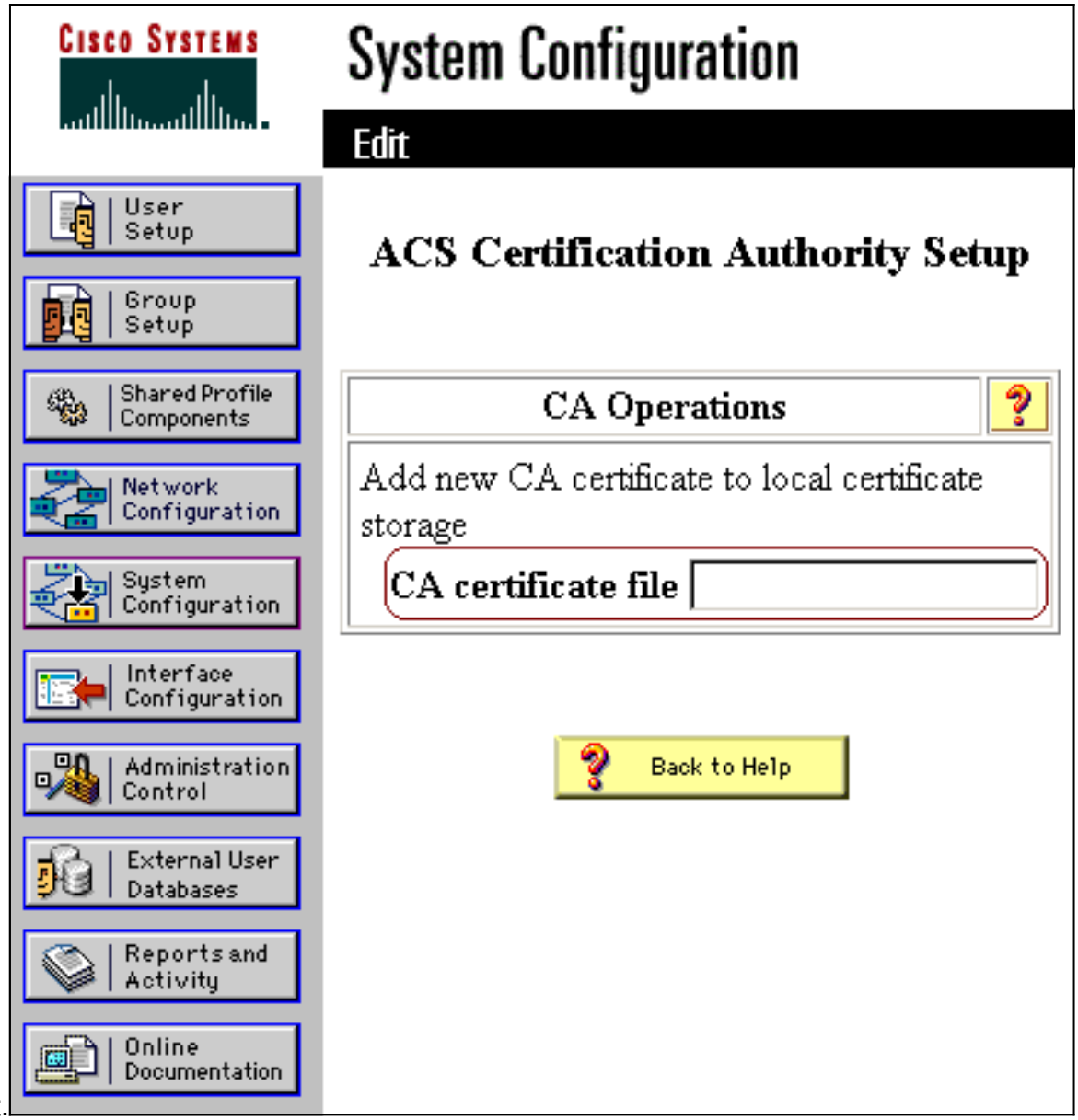


vez.

Especifique as autoridades de certificado adicionais em que o ACS deve confiar

O ACS confia automaticamente CA que emitiu seu próprio certificado. Se os certificados de cliente são emitidos por CA adicionais, você deve terminar estas etapas:

1. Clique em System Configuration e, em seguida, em ACS Certificate Setup.
2. Clique em ACS Certificate Authority Setup para adicionar CAs à lista de certificados confiáveis.
3. No campo para o arquivo do certificado de CA, digite a localização do certificado e, em seguida, clique em



Submit.

4. Clique em Edit Certificate Trust List.
5. Selecione todas as CAs nas quais o ACS deve confiar e desmarque todas as CAs nas quais o ACS não deve confiar.
6. Clique em

Submit.

Reiniciar o serviço e definir as configurações EAP-TLS no ACS

Termine estas etapas a fim reiniciar o serviço e configurar ajustes do EAP-TLS:

1. Clique em System Configuration e, depois, em Service Control.
2. Clique o **reinício** a fim reiniciar o serviço.
3. A fim configurar ajustes do EAP-TLS, clique a **configuração de sistema**, e clique então a **instalação da autenticação global**.
4. Marque Allow EAP-TLS e, em seguida, marque uma ou mais comparações de certificado.
5. Clique em