Secure ACS pour Windows v3.2 avec l'authentification de machine d'EAP-TLS

Contenu

Introduction

Ce document décrit comment configurer Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) avec le Système de contrôle d'accès sécurisé Cisco (ACS) pour la version 3.2 de Windows.

Remarque: L'authentification de machine n'est pas prise en charge avec l'Autorité de certification (CA) de Novell. ACS peut employer l'EAP-TLS pour prendre en charge l'authentification de machine au Répertoire actif de Microsoft Windows. Le client d'utilisateur final pourrait limiter le protocole pour l'authentification de l'utilisateur au même protocole qui est utilisé pour l'authentification de machine. C'est-à-dire, l'utilisation de l'EAP-TLS pour l'authentification de machine pourrait exiger l'utilisation de l'EAP-TLS pour l'authentification de l'utilisateur. Pour plus

d'informations sur l'authentification de machine, référez-vous à la section d'authentification de machine du *guide utilisateur pour le Cisco Secure Access Control Server 4.1*.

Remarque: En installant ACS pour authentifier des ordinateurs par l'intermédiaire de l'EAP-TLS et de l'ACS a été installé pour l'authentification de machine, le client doit être configuré pour faire l'authentification de machine seulement. Le pour en savoir plus, se réfèrent comment activer l'authentification ordinateur ordinateur pour un réseau 802.1X-based dans les Windows Vista, dans les Windows Server 2008, et dans les Windows XP Service Pack 3.

Conditions préalables

Conditions requises

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Cisco Secure ACS pour la version 3.2 de Windows
- Services de certificat de Microsoft (installés en tant qu'autorité de certification de racine d'entreprise [CA])**Remarque:** Le pour en savoir plus, se rapportent au guide pas à pas d'installer une autorité de certification .
- Service DNS avec le Windows 2000 Server avec le Service Pack 3 et le correctif 323172**Remarque:** Si vous rencontrez des problèmes serveurs CA, installez le correctif 323172 . Le client du Windows 2000 SP3 exige du correctif 313664 d'activer l'authentification de 802.1x d'IEEE.
- Point d'accès Sans fil 12.01T de Gamme Cisco Aironet 1200
- Windows XP Professionnel courant du ThinkPad T30 IBM avec le Service Pack 1

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Théorie générale

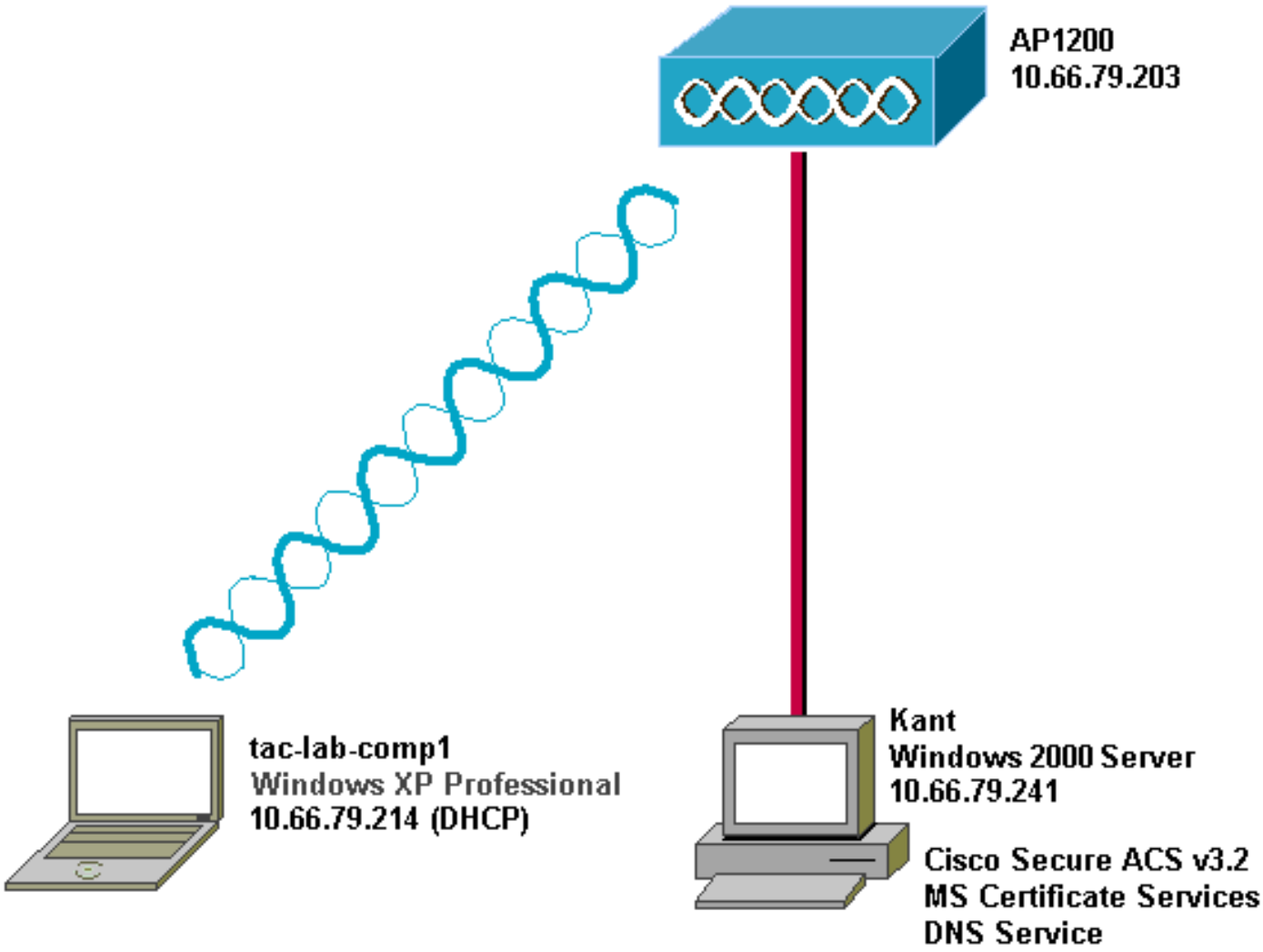
L'EAP-TLS et le Protected Extensible Authentication Protocol (PEAP) construisent et utilisent un tunnel TLS/Secure Socket Layer (SSL). L'EAP-TLS utilise l'authentification mutuelle dans laquelle le serveur et les clients ACS (authentification, autorisation, et comptabilité [AAA]) ont des Certificats et prouvent leurs identités entre eux. Le PEAP, cependant, utilise seulement l'authentification de côté serveur ; seulement le serveur a un certificat et prouve son identité au client.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :



Configurer le Cisco Secure ACS pour Windows v3.2

Suivez les étapes ci-dessous pour configurer ACS 3.2.

1. Obtenez un certificat pour le serveur ACS.
2. Configurez ACS pour utiliser un certificat de mémoire.
3. Spécifiez les autorités de certification supplémentaires aux lesquelles l'ACS devrait faire confiance.
4. Redémarrez le service et configurez les configurations PEAP sur l'ACS.
5. Spécifiez et configurez le Point d'accès en tant que client d'AAA.
6. Configurez les bases de données d'utilisateur externe.
7. Redémarrez le service.

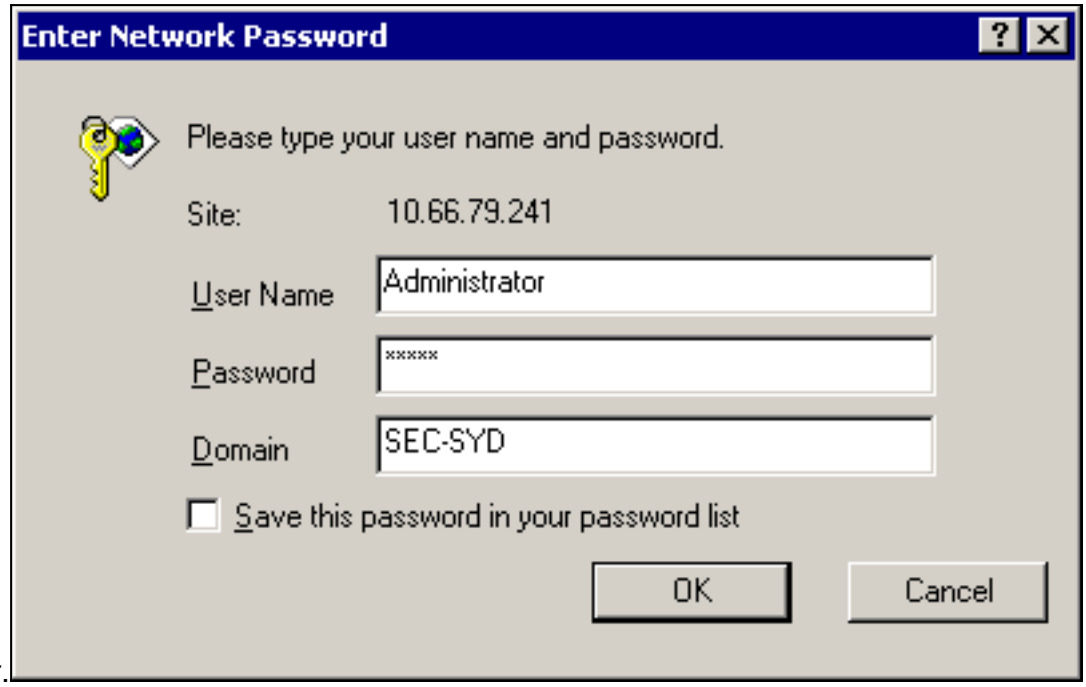
Obtenez un certificat pour le serveur ACS

Suivez ces étapes pour obtenir un certificat.

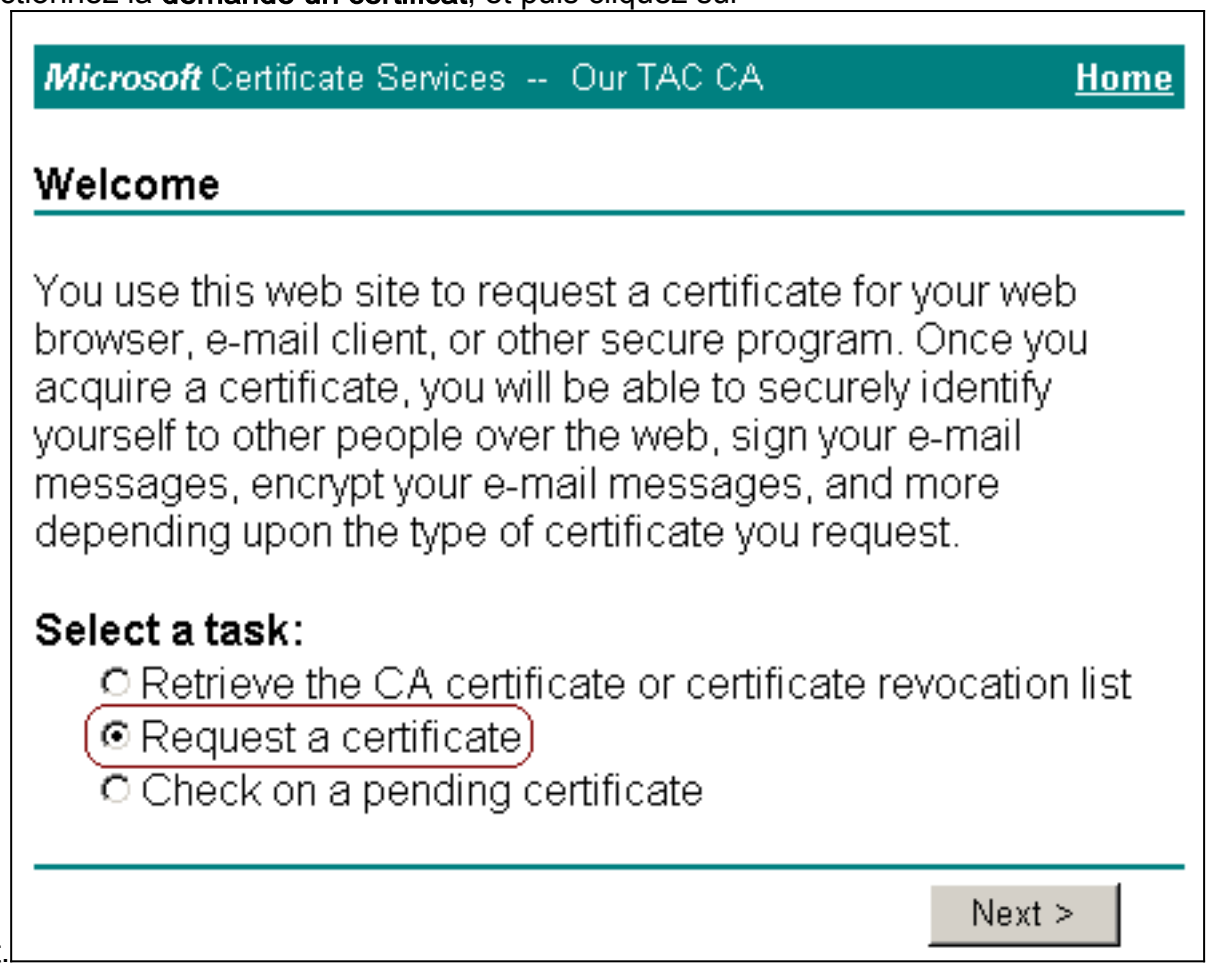
1. Sur le serveur ACS, ouvrez un navigateur Web, et entrez dans **http:// CA-ip-address/certsrv**

afin d'accéder au serveur CA.

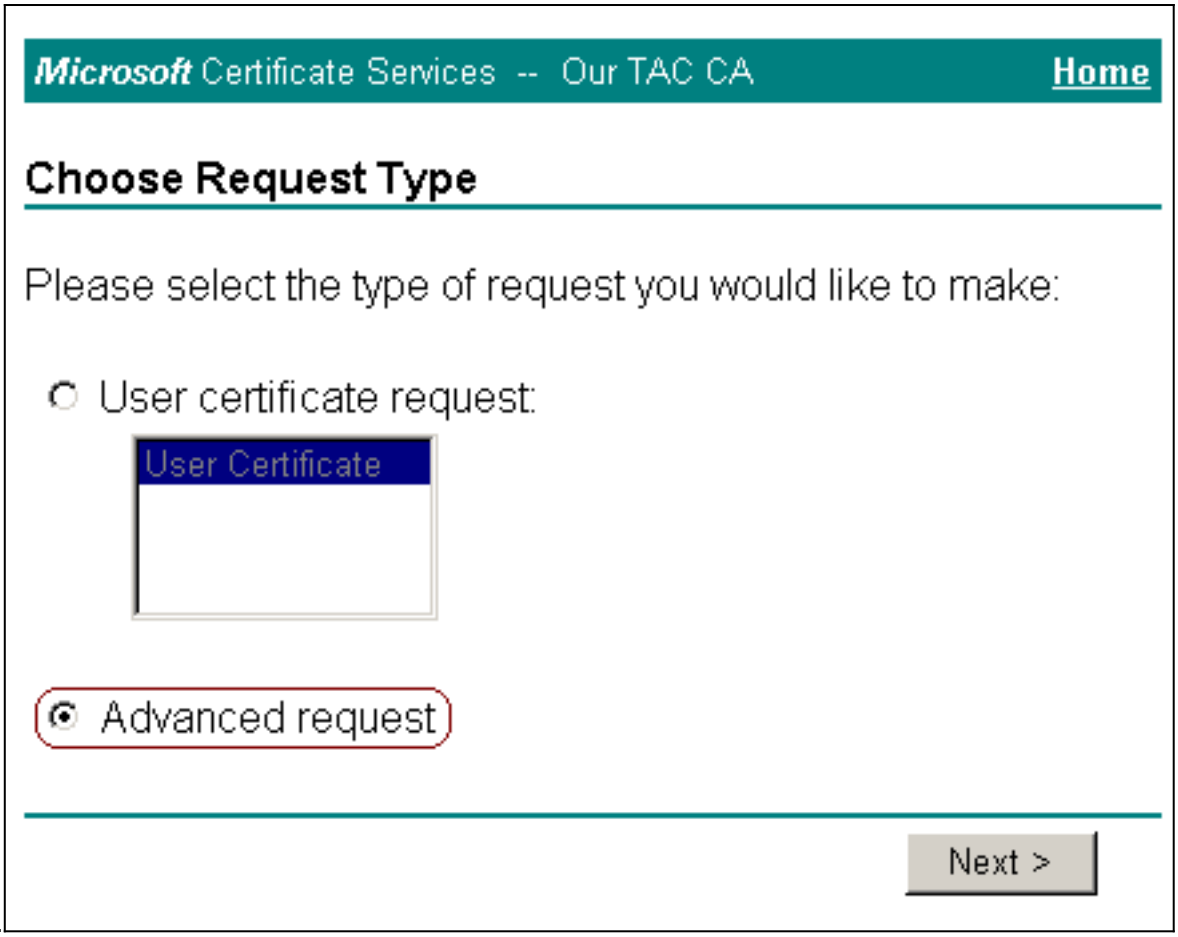
2. Procédure de connexion au domaine comme administrateur.



3. Sélectionnez la **demande un certificat**, et puis cliquez sur Next.

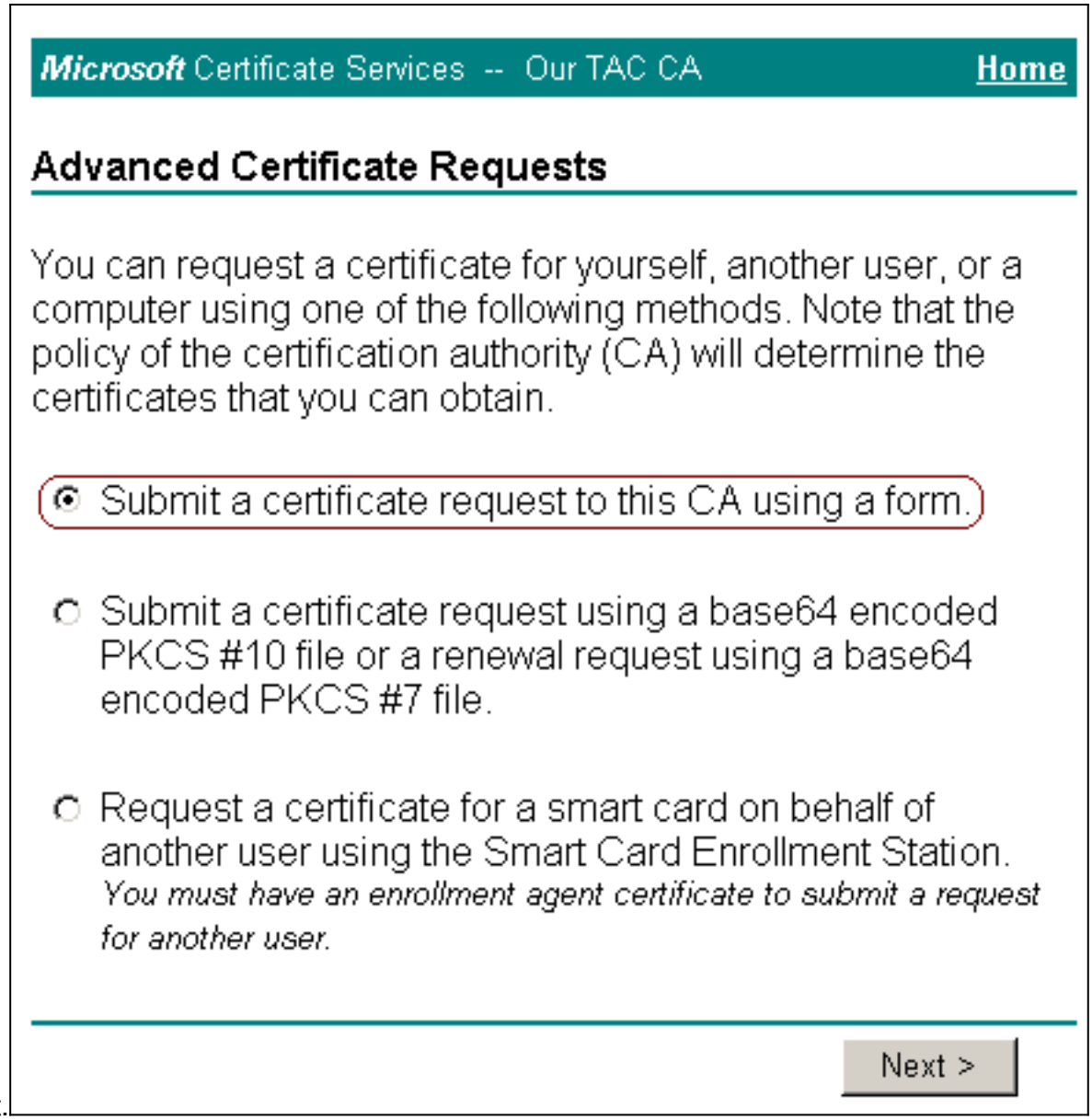


4. **La demande avancée** choisie, et cliquent sur Next



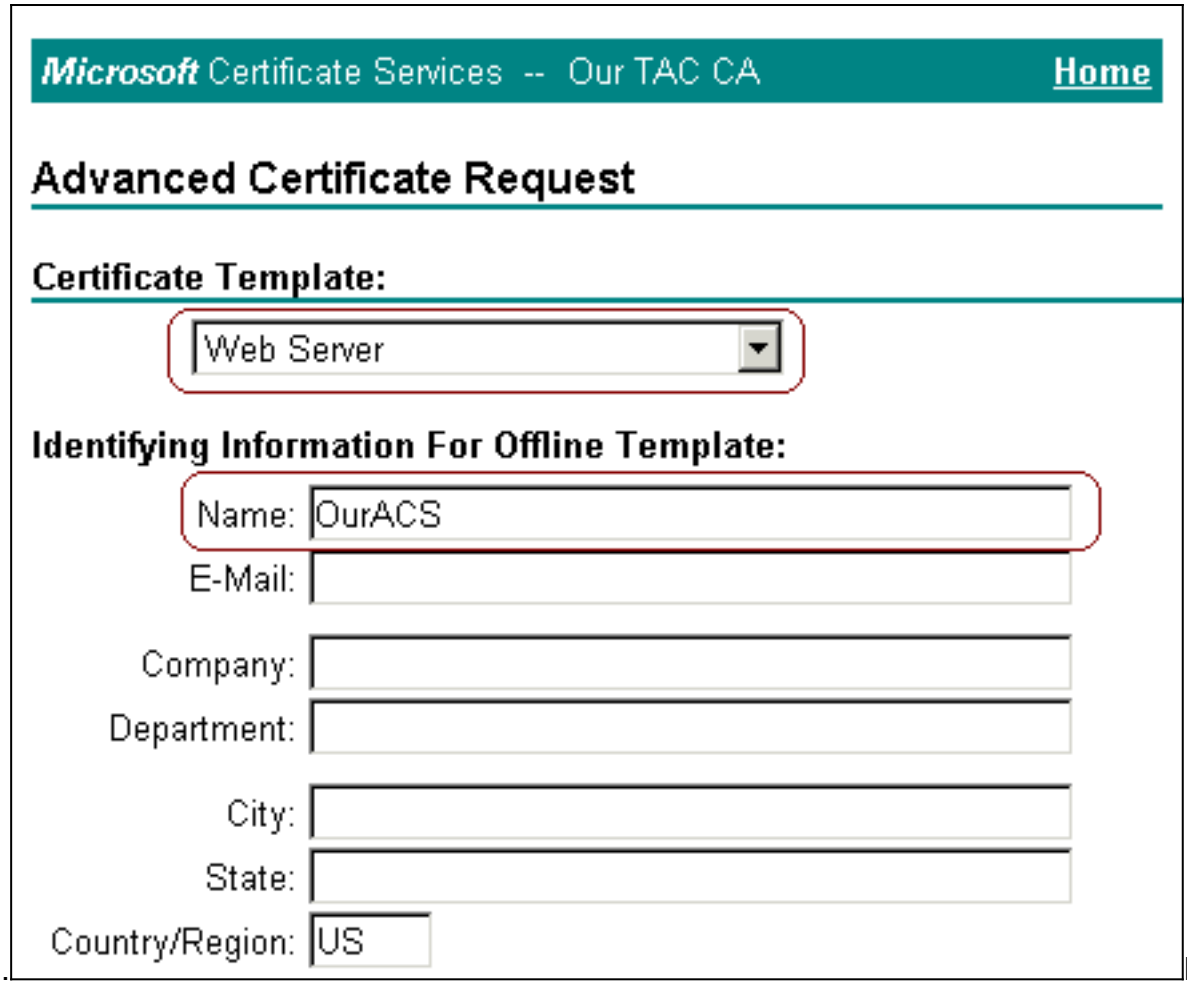
alors.

5. Choisi **soumettez une demande de certificat à ce CA utilisant une forme**, et puis cliquez sur

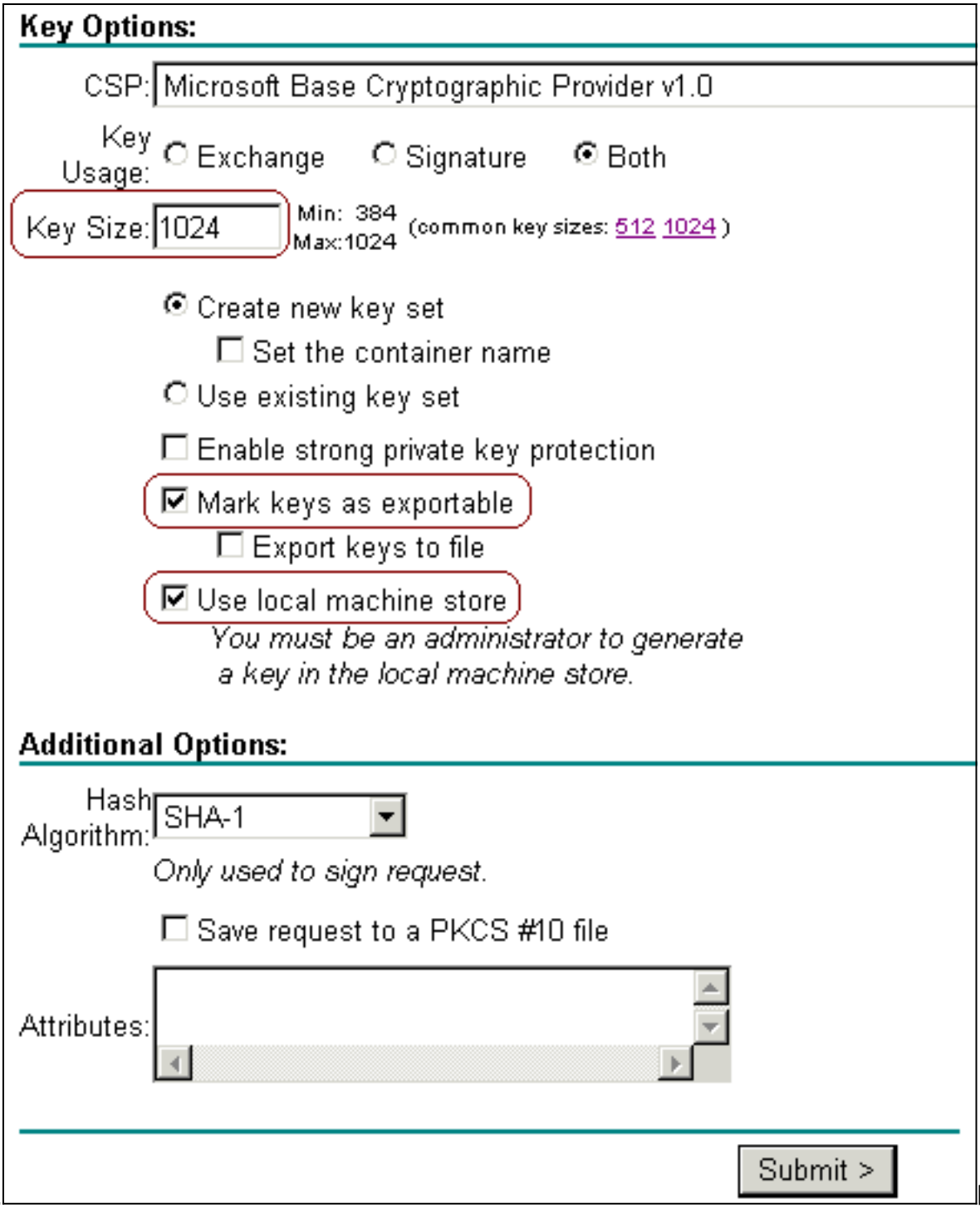


Next.

6. Configurez les options de certificat :**Le serveur Web** choisi comme modèle de certificat, et écrivent le nom du serveur



ACS.Écriv ez **1024** dans le domaine de taille de clé, et vérifiez les **clés de marque en tant que** cases **exportables** et d'**utilisation d'ordinateur local de mémoire**.Configurez d'autres options comme nécessaire, et puis cliquez sur



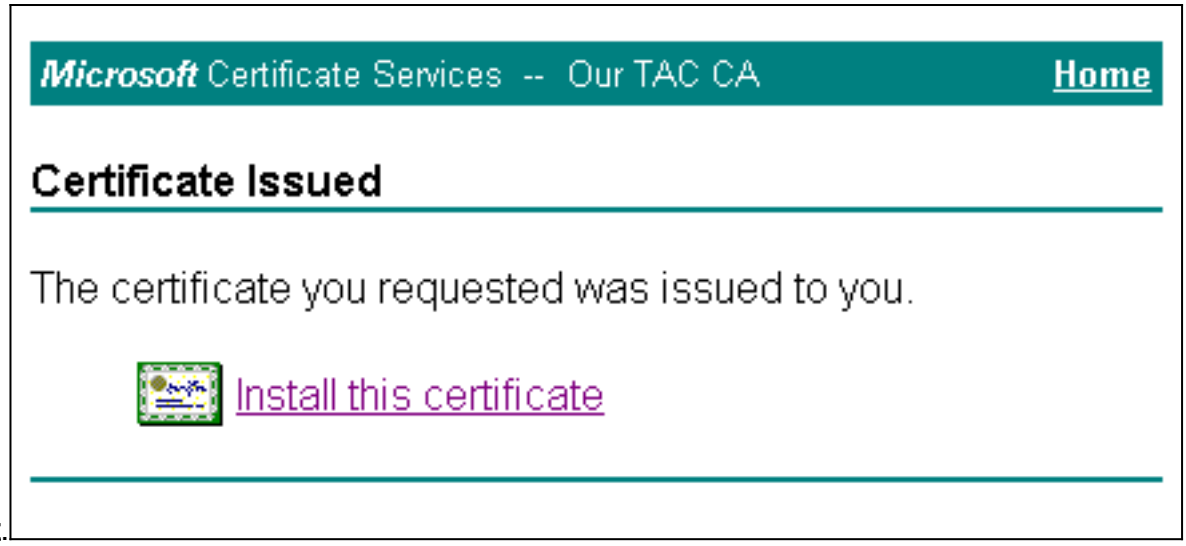
Submit.**R**

emarque: Si la boîte de dialogue potentielle de violation de script apparaît, cliquez sur **oui**

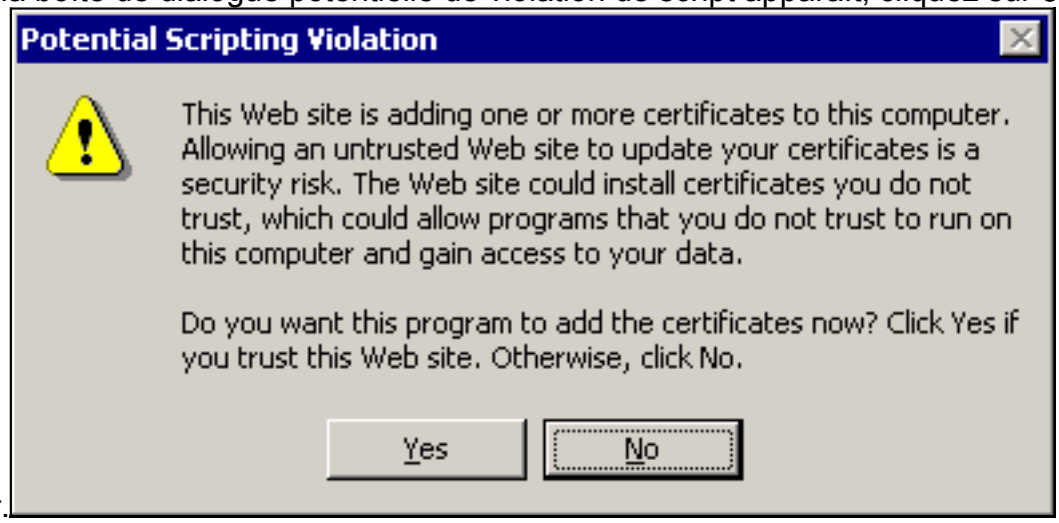
pour continuer.

7. Le clic **installent ce**

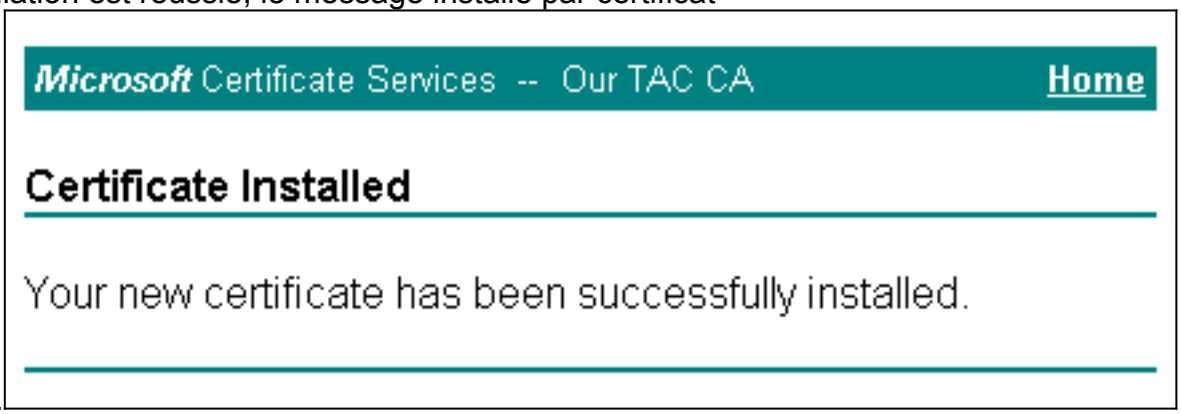
certificat.



Remarque: Si la boîte de dialogue potentielle de violation de script apparaît, cliquez sur **oui** pour continuer.



8. Si l'installation est réussie, le message installé par certificat apparaît.



Configurez ACS pour utiliser un certificat de mémoire

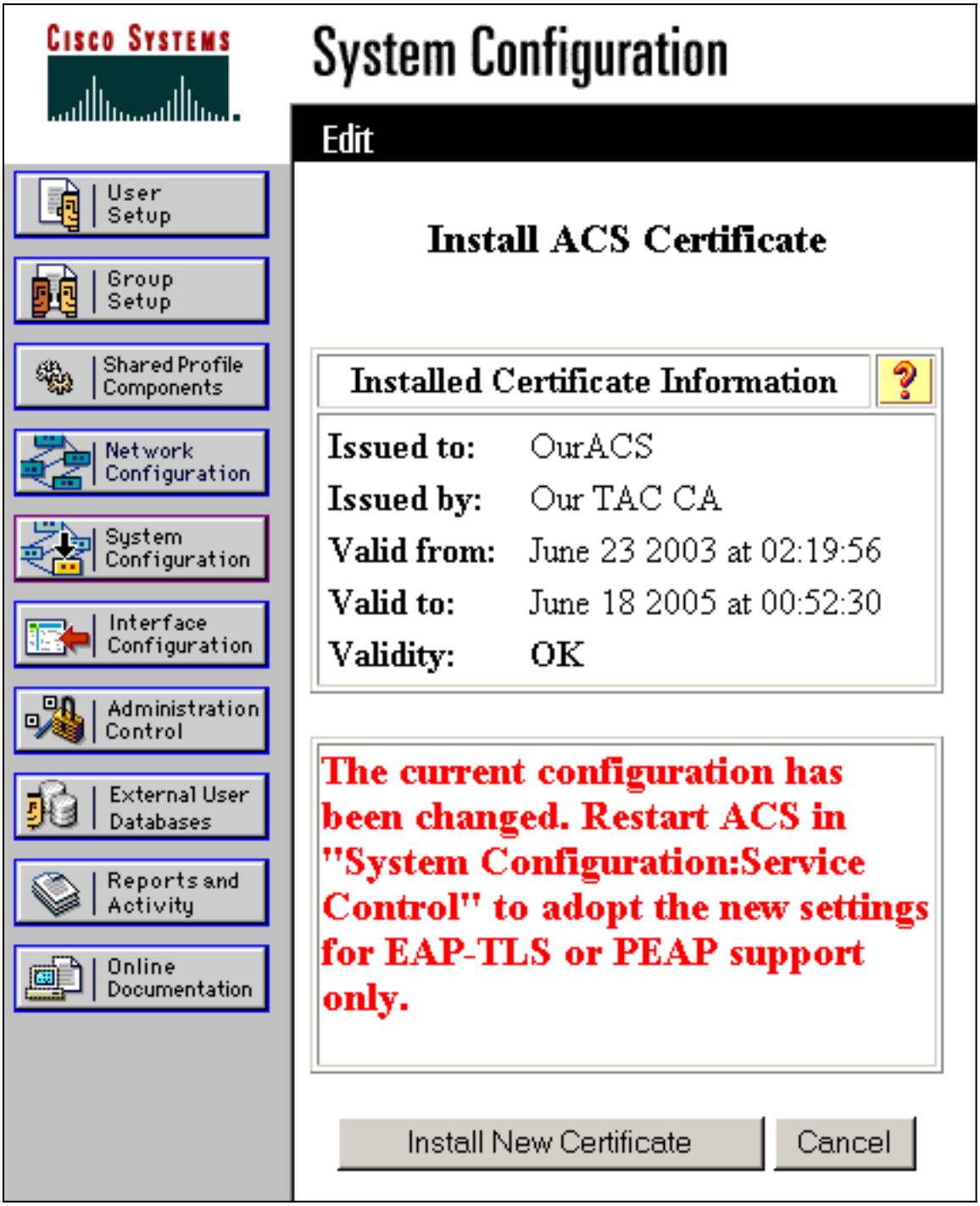
Terminez-vous ces étapes afin de configurer ACS pour utiliser le certificat dans la mémoire.

1. Ouvrez un navigateur Web, et entrez dans **http:// *ACS-ip-address:2002/*** afin d'accéder au serveur ACS.
2. Cliquez sur la **configuration système**, et puis cliquez sur l'**installation de certificat ACS**.
3. Le clic **installent le certificat ACS**.
4. Cliquez sur le **certificat d'utilisation de la** case d'option de **mémoire**.
5. Dans le domaine NC de certificat, écrivez le nom du certificat que vous avez assigné dans

l'étape 5a d'[obtenir un certificat de l'ACS Serversection de](#) ce document.

6. Cliquez sur **Submit**.

Une fois que la configuration est complète, un message de confirmation apparaît qui indique que la configuration du serveur ACS a été changée.**Remarque:** Vous n'avez pas besoin de redémarrer l'ACS à ce

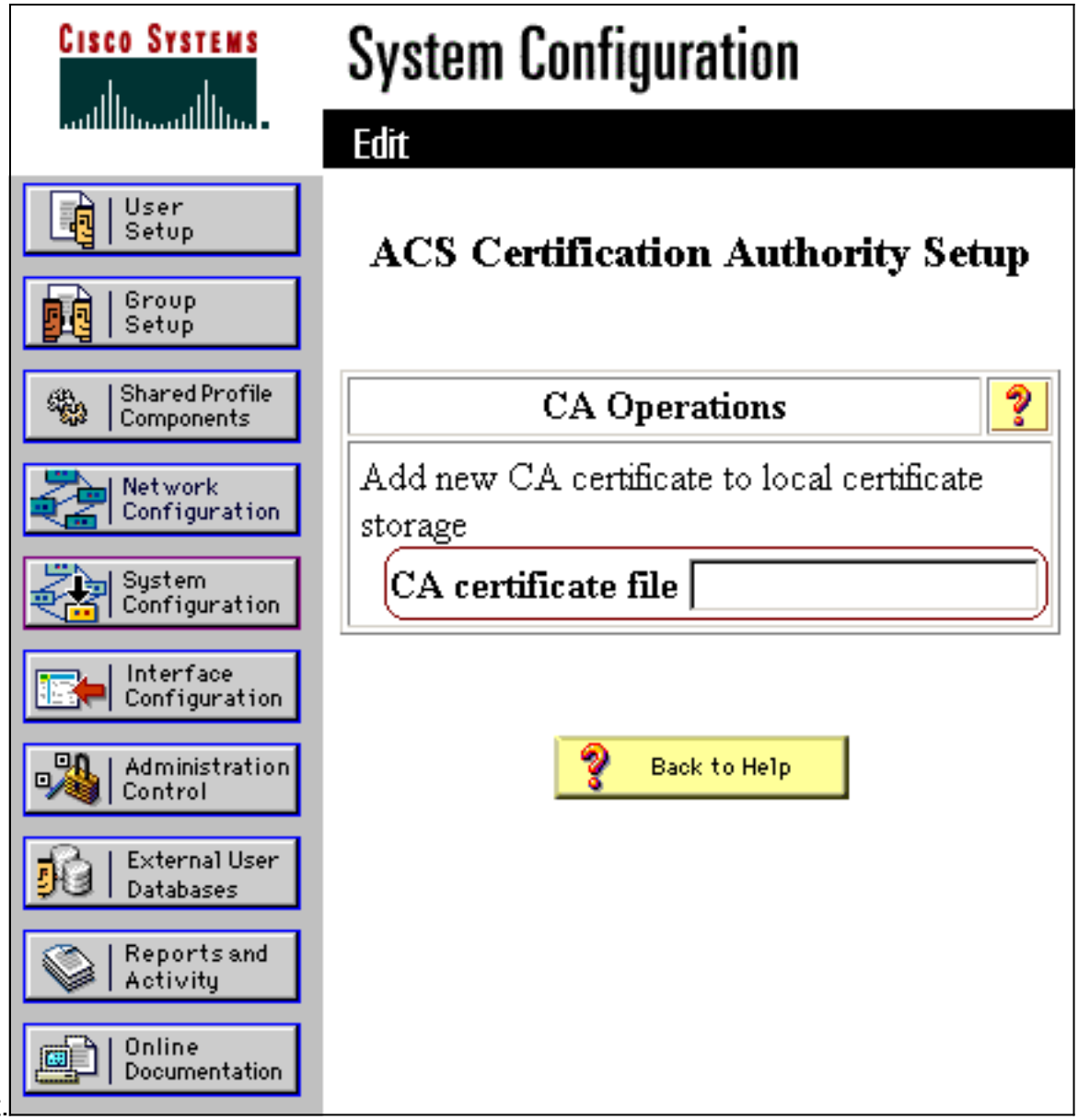


moment.

Spécifiez les autorités de certification supplémentaires aux lesquelles l'ACS devrait faire confiance

L'ACS fait confiance automatiquement au CA qui a délivré son propre certificat. Si les certificats client sont délivrés par CAs supplémentaire, vous devez se terminer ces étapes :

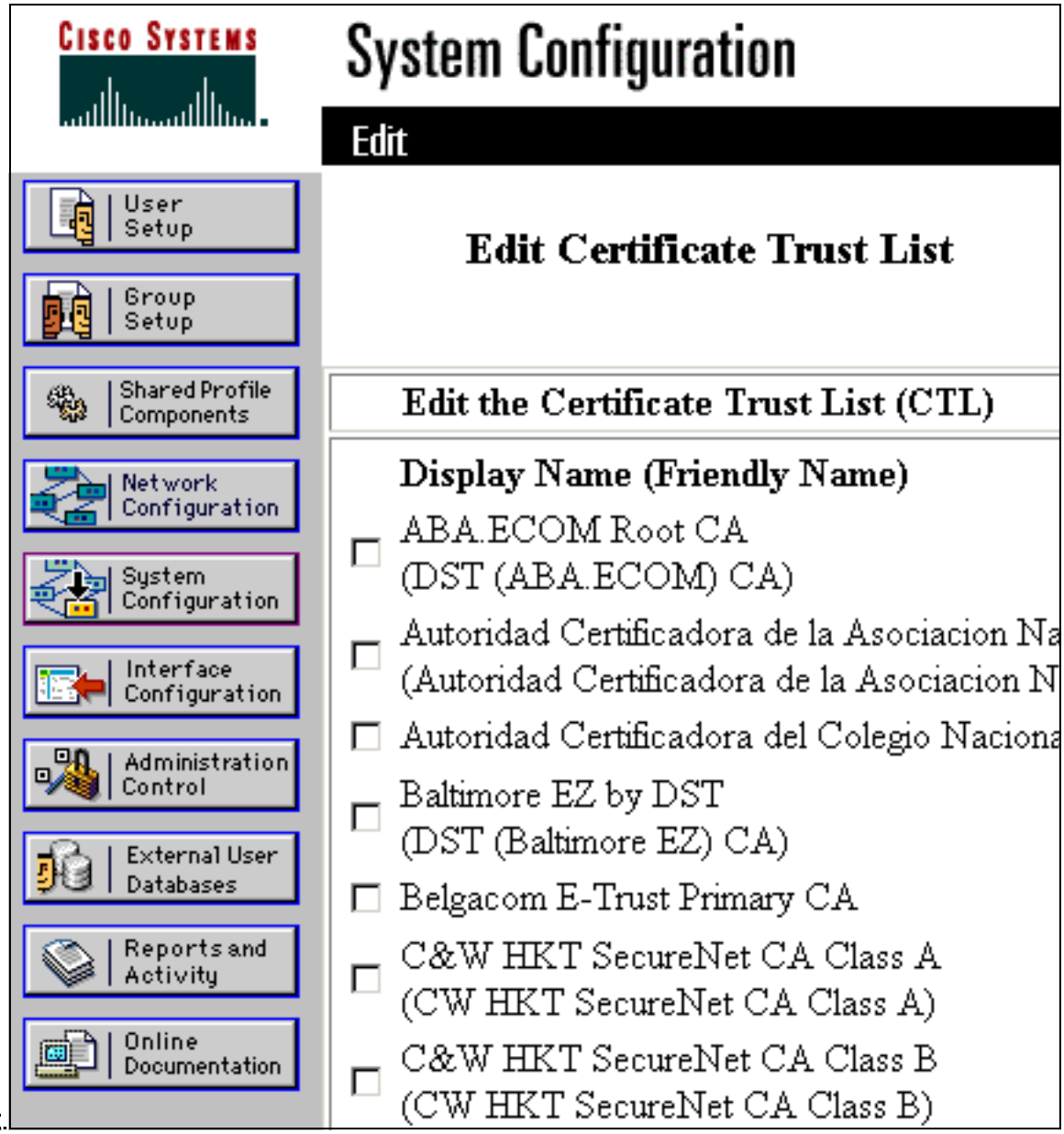
1. Cliquez sur la **configuration système**, et puis cliquez sur l'**installation de certificat ACS**.
2. Cliquez sur l'**installation d'autorité de certification ACS** pour ajouter le CAs à la liste de Certificats de confiance.
3. Dans le domaine pour le fichier de certificat de CA, entrez l'emplacement du certificat, et puis cliquez sur



Submit.

4. Cliquez sur Edit la **liste de confiance de certificat**.
5. Vérifiez tout le CAs au lequel l'ACS devrait faire confiance, et décochez tout le CAs au lequel l'ACS ne devrait pas faire confiance.
6. Cliquez sur

Submit.



Redémarrez le service et configurez les configurations d'EAP-TLS sur l'ACS

Terminez-vous ces étapes afin de redémarrer le service et configurer des configurations d'EAP-TLS :

1. **La configuration système de** clic, et cliquent sur alors le **contrôle des services**.
2. **Reprise de** clic afin de redémarrer le service.
3. Afin de configurer des configurations d'EAP-TLS, la **configuration système de** clic, et puis cliquer sur l'**installation globale d'authentification**.
4. Vérifiez **permettent l'EAP-TLS**, et puis vérifient un ou plusieurs des comparaisons de certificat.
5. Cliquez sur