Configuration de l'accélérateur de contenu sécurisé Cisco Secure pour Windows v3.2 avec authentification PEAP-MS-CHAPv2

Contenu

Introduction

Ce document explique comment configurer le Protected Extensible Authentication Protocol (PEAP) avec le Cisco Secure ACS pour la version 3.2 de Windows.

Pour plus d'informations sur la façon configurer sécurisez l'accès Sans fil utilisant les contrôleurs LAN Sans fil, logiciel de Microsoft Windows 2003, et le Cisco Secure Access Control Server (ACS) 4.0, se rapportent au PEAP sous des réseaux sans fil unifié avec ACS 4.0 et Windows 2003.

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**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

Le PEAP et l'EAP-TLS construisent et utilisent un tunnel TLS/Secure Socket Layer (SSL). Le PEAP utilise seulement l'authentification de côté serveur ; seulement le serveur a un certificat et prouve son identité au client. L'EAP-TLS, cependant, 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.

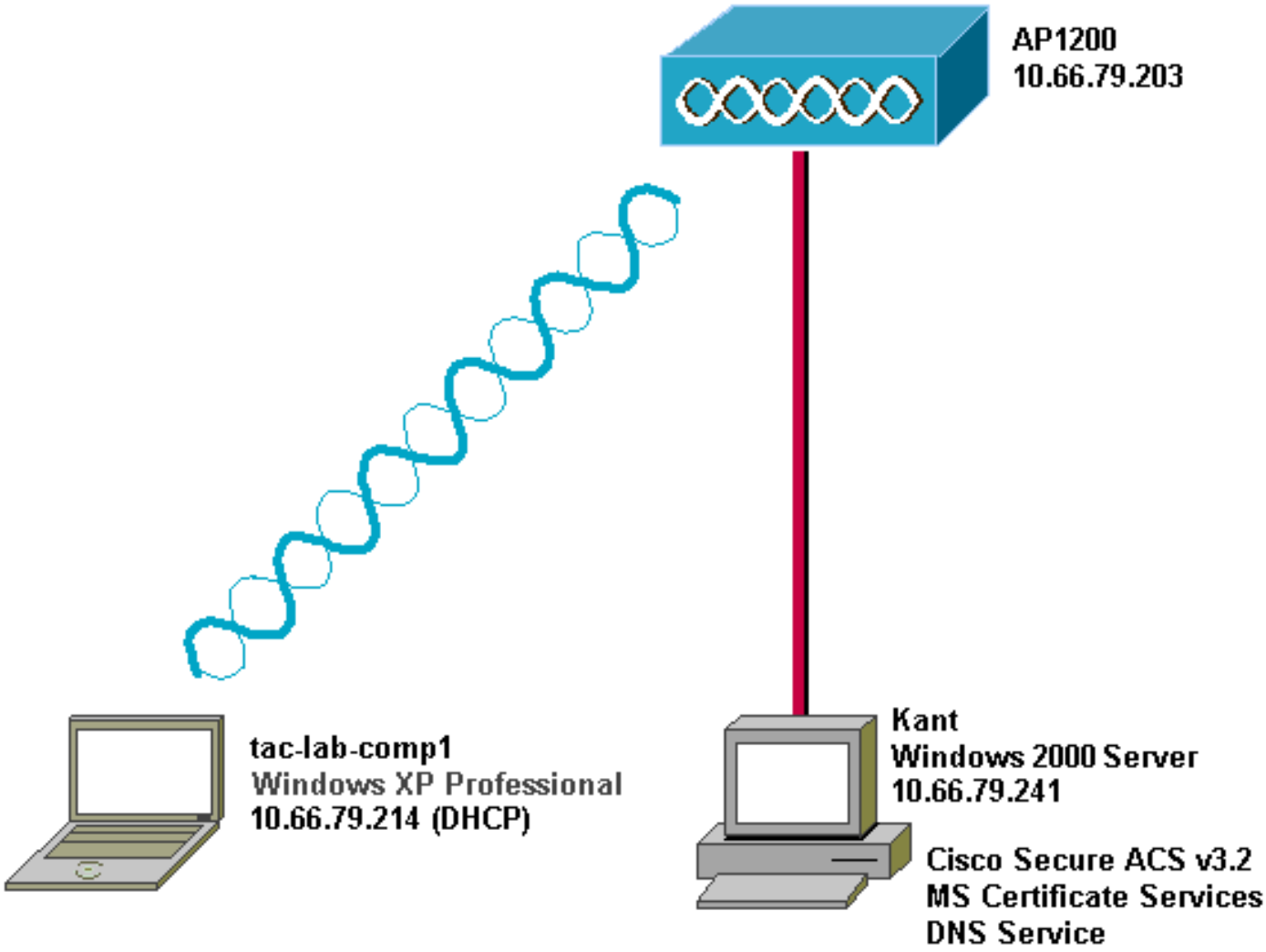
Le PEAP est commode parce que les clients n'ont pas besoin des Certificats. L'EAP-TLS est utile pour authentifier les périphériques sans tête, parce que les Certificats n'exigent aucune interaction utilisateur.

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 :



Configurez le Cisco Secure ACS pour Windows v3.2

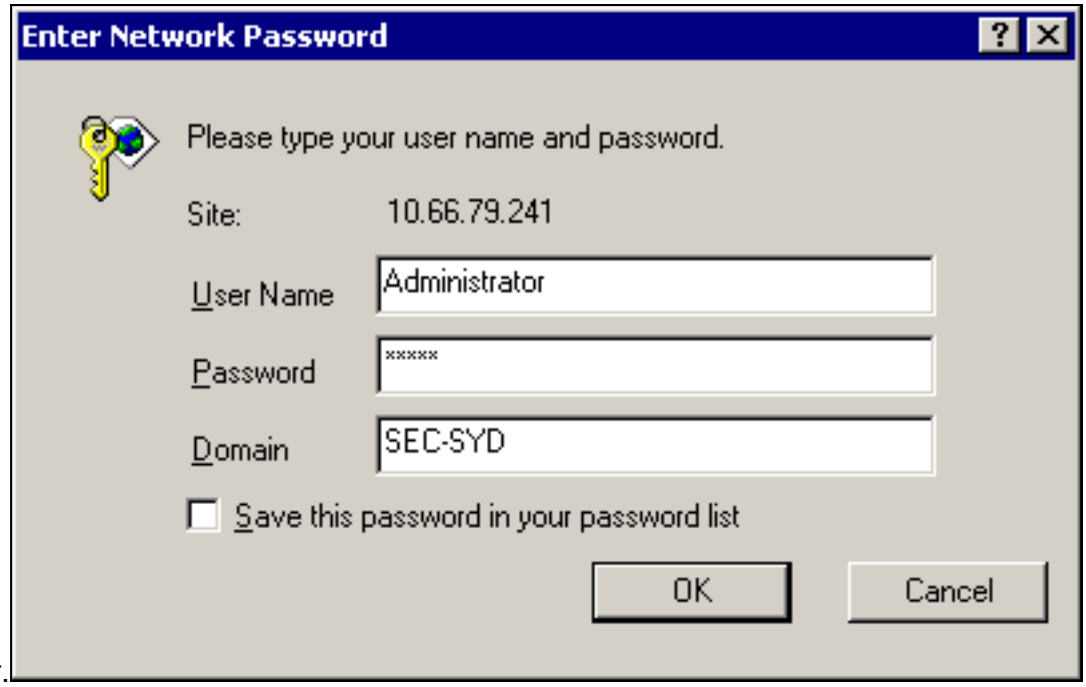
Suivez ces étapes pour configurer ACS 3.2.

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

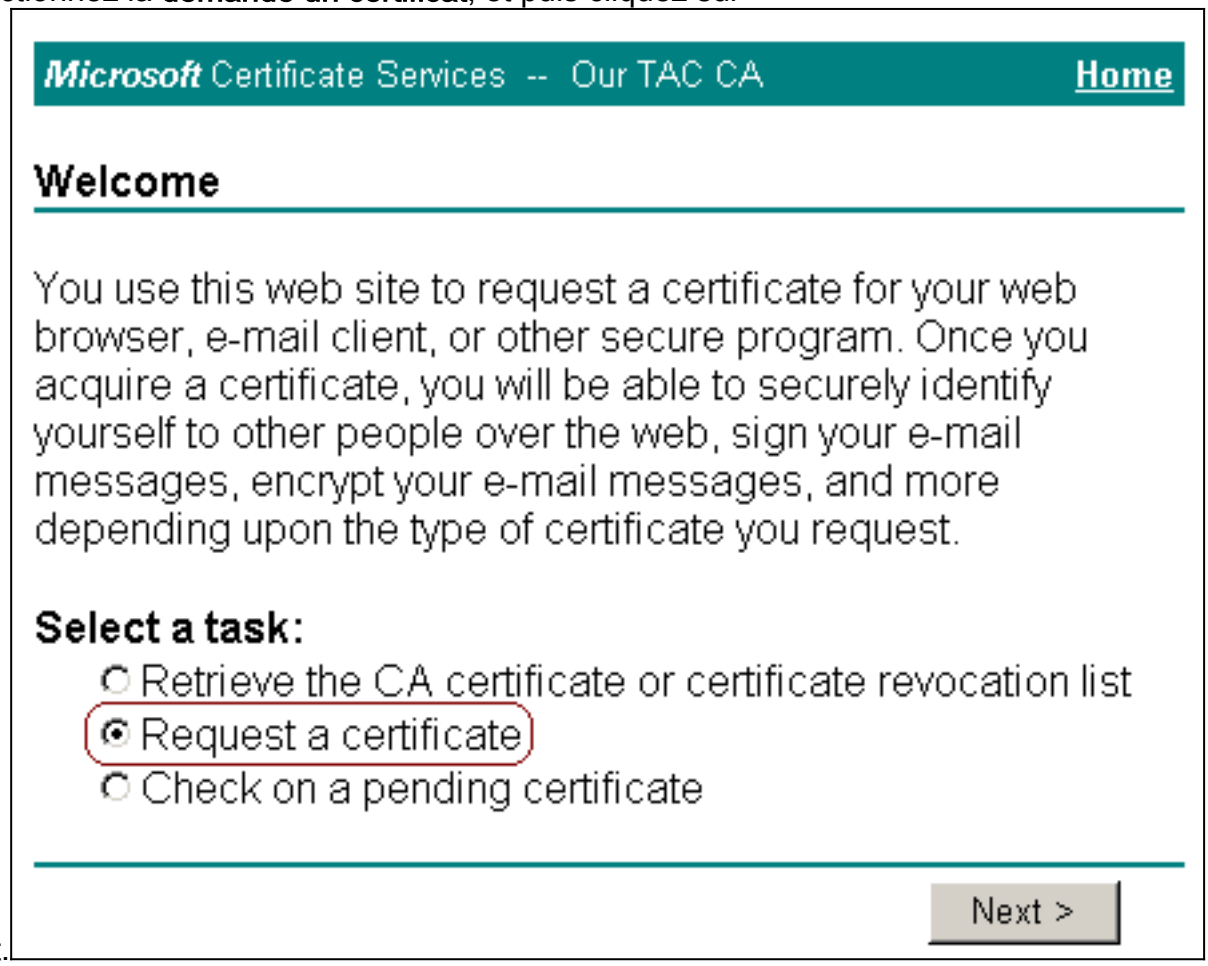
Suivez ces étapes pour obtenir un certificat.

1. Sur le serveur ACS, ouvrez un navigateur Web et parcourez au serveur CA en entrant dans **http:// CA-ip-address/certsrv** dans la barre d'adresses. Procédure de connexion au domaine comme



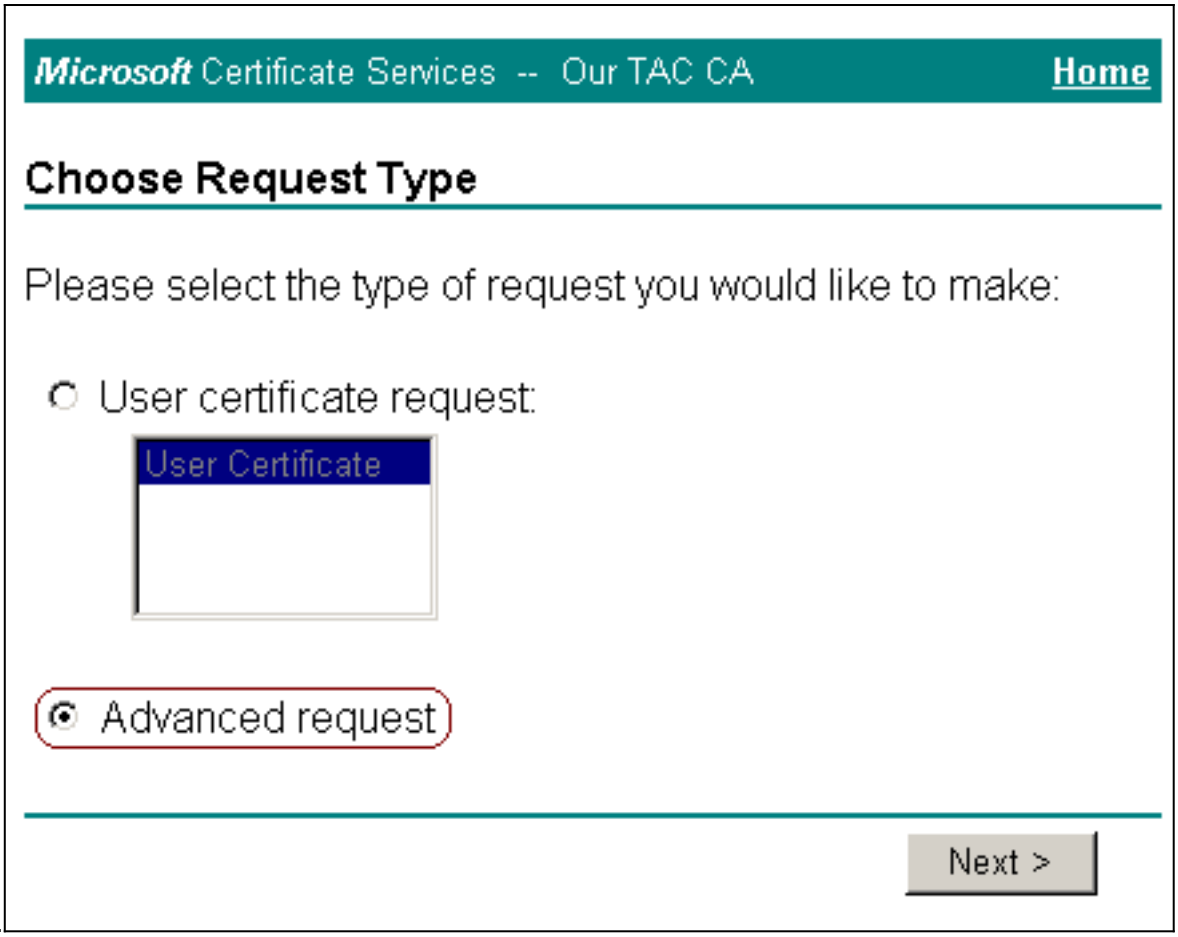
administrateur.

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



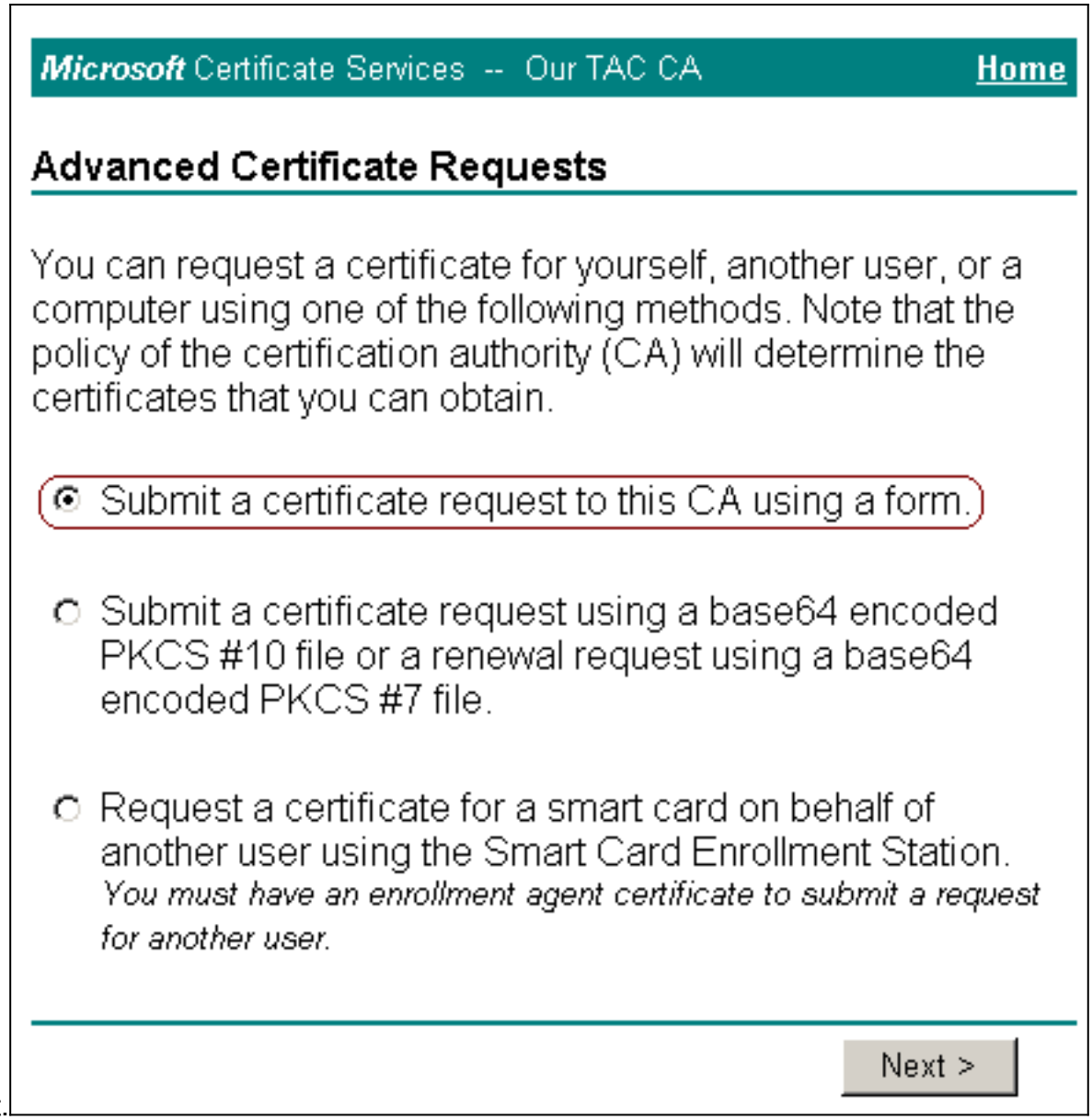
Next.

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



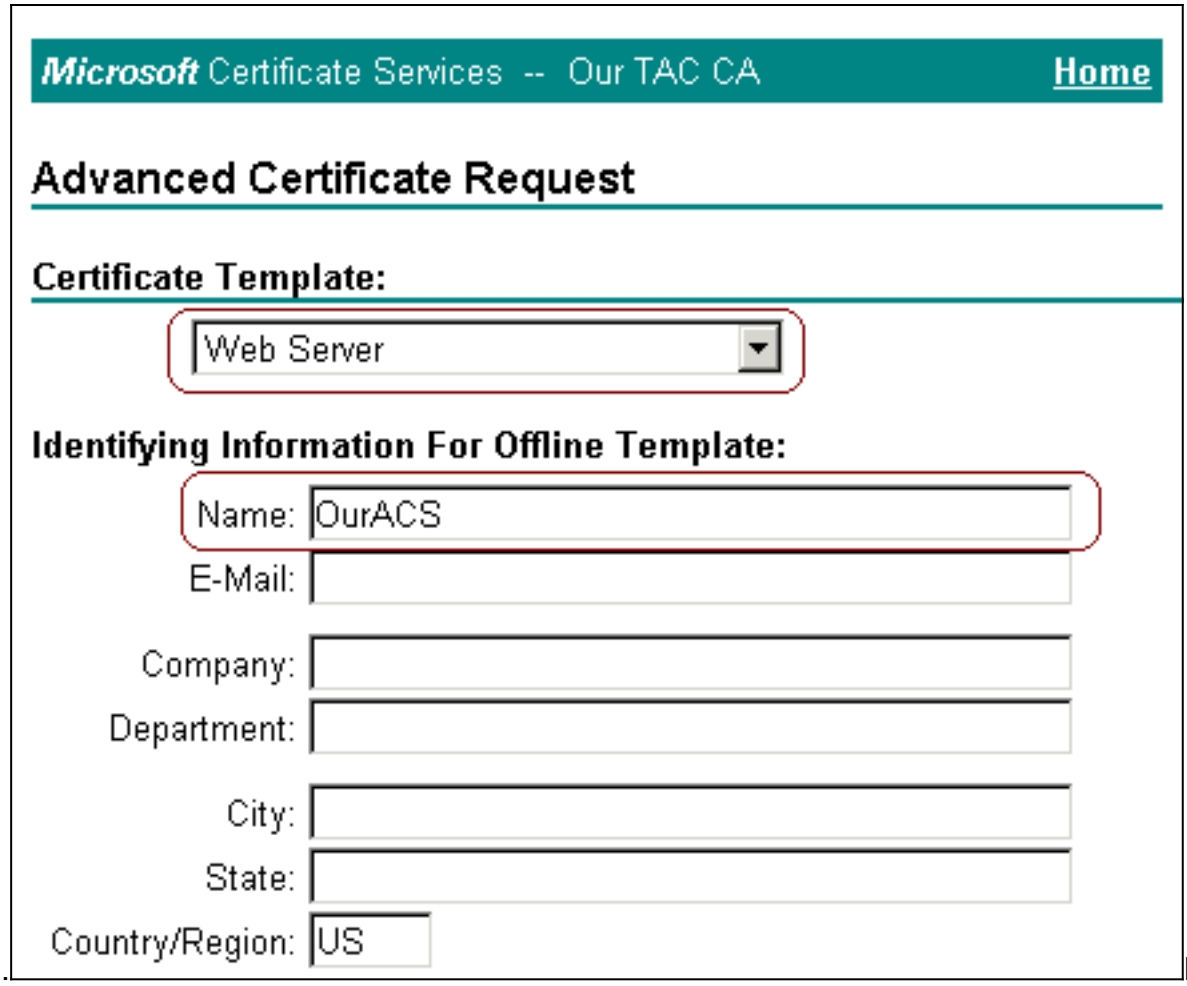
alors.

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

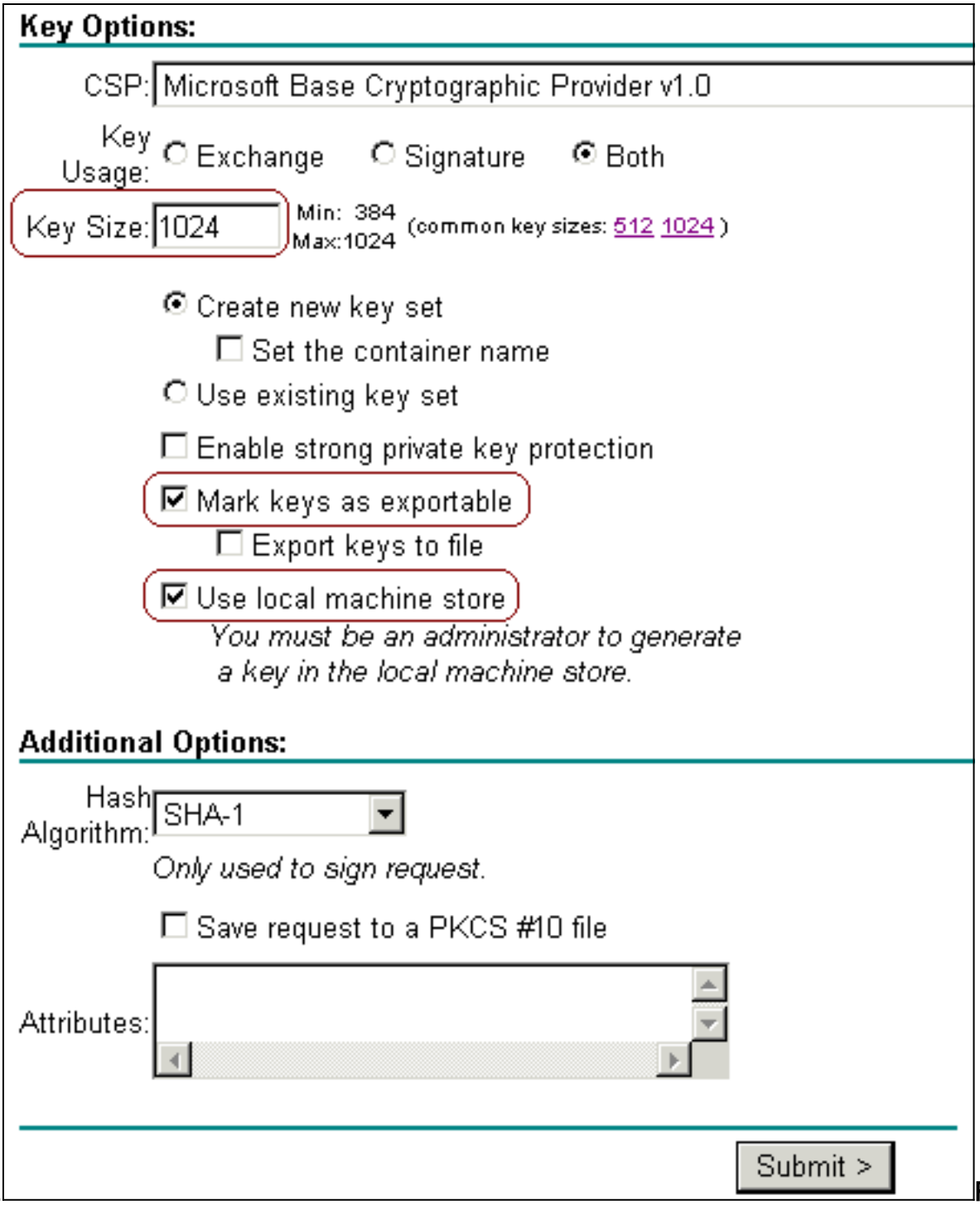


Next.

5. Configurez les options de certificat.**Serveur Web** choisi comme modèle de certificat. Écrivez le nom du serveur



ACS.Fixez la taille de clé à **1024**. Sélectionnez les options pour des **clés de marque en tant que mémoire exportable** et d'**utilisation d'ordinateur local**. Configurez d'autres options comme nécessaire, et puis cliquez sur

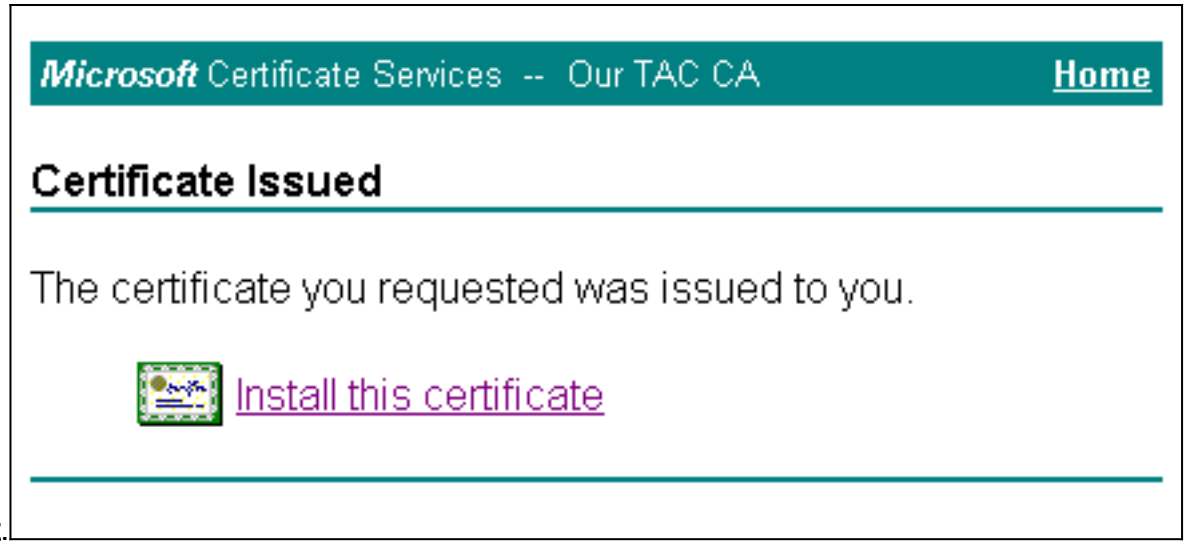


Submit.**R**

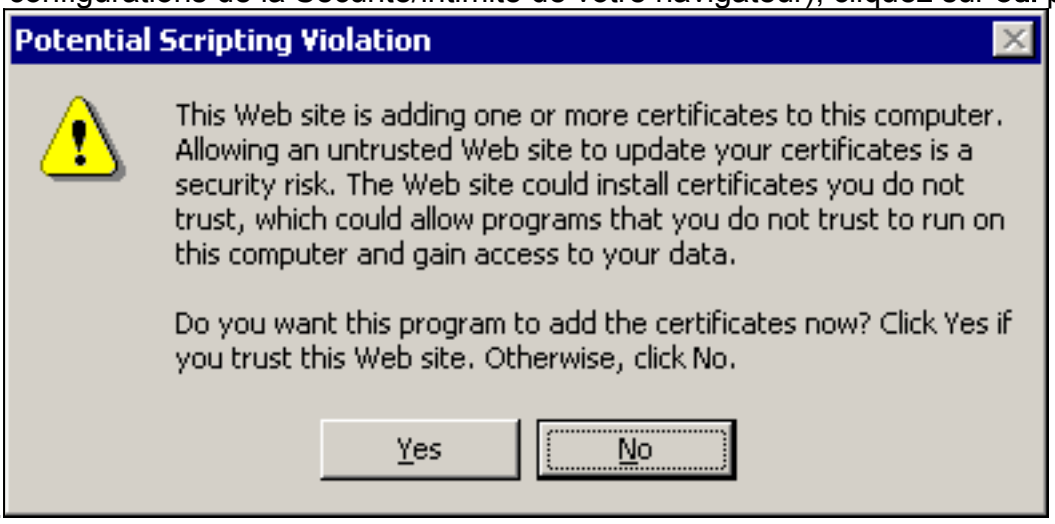
emarque: Si vous voyez une fenêtre d'avertissement se référant à une violation de script (selon les configurations de la Sécurité/intimité de votre navigateur), cliquez sur **oui** pour continuer.

6. Le clic **installent ce**

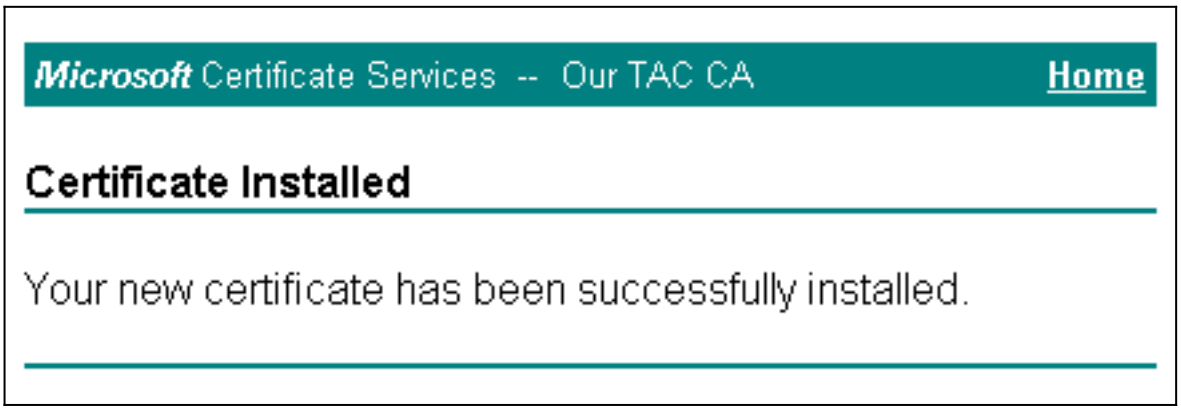
certificat.



Remarque: Si vous voyez une fenêtre d'avertissement se référant à une violation de script (selon les configurations de la Sécurité/intimité de votre navigateur), cliquez sur **oui** pour continuer.



7. Si l'installation a été réussie, vous verrez un message de confirmation.

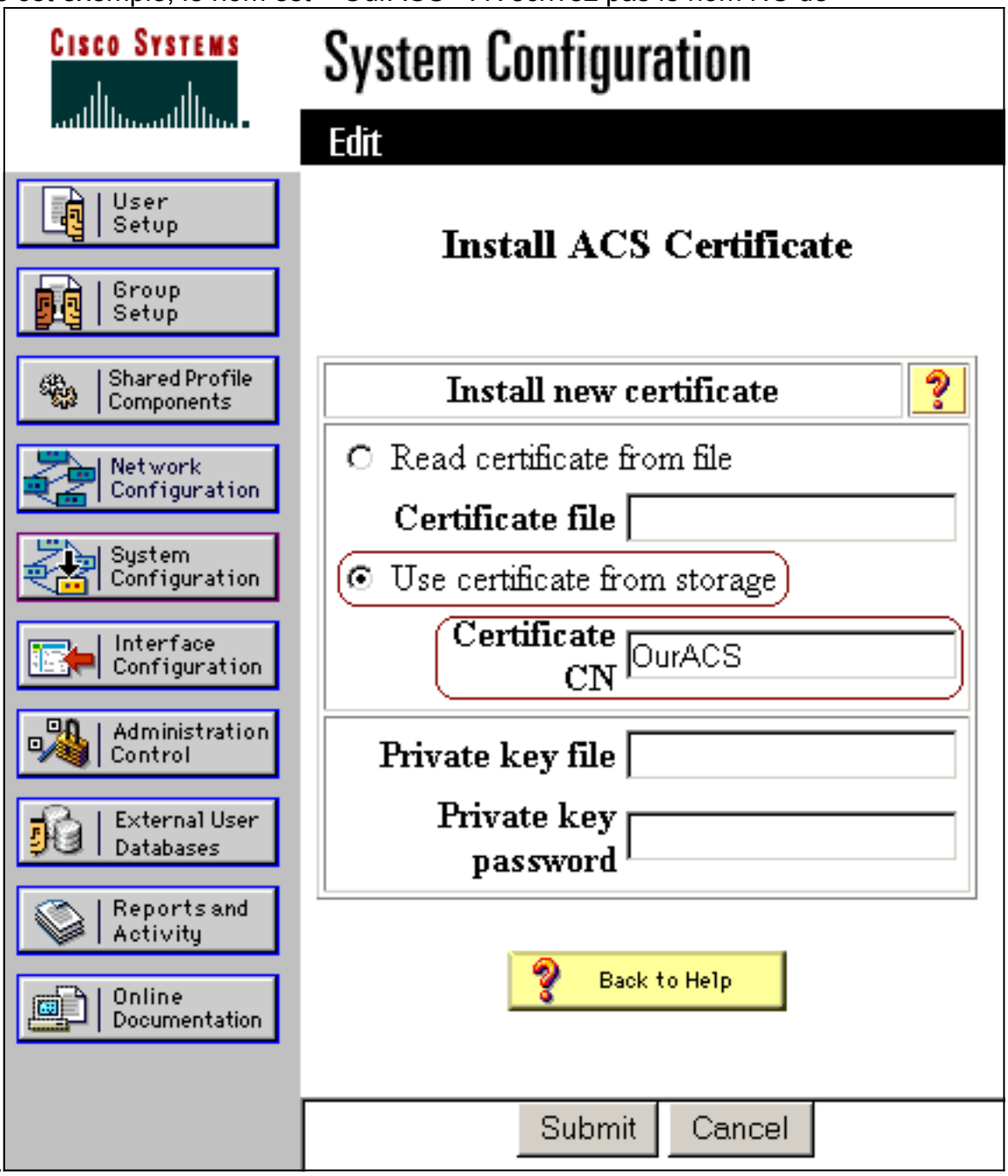


Configurez ACS pour utiliser un certificat de mémoire

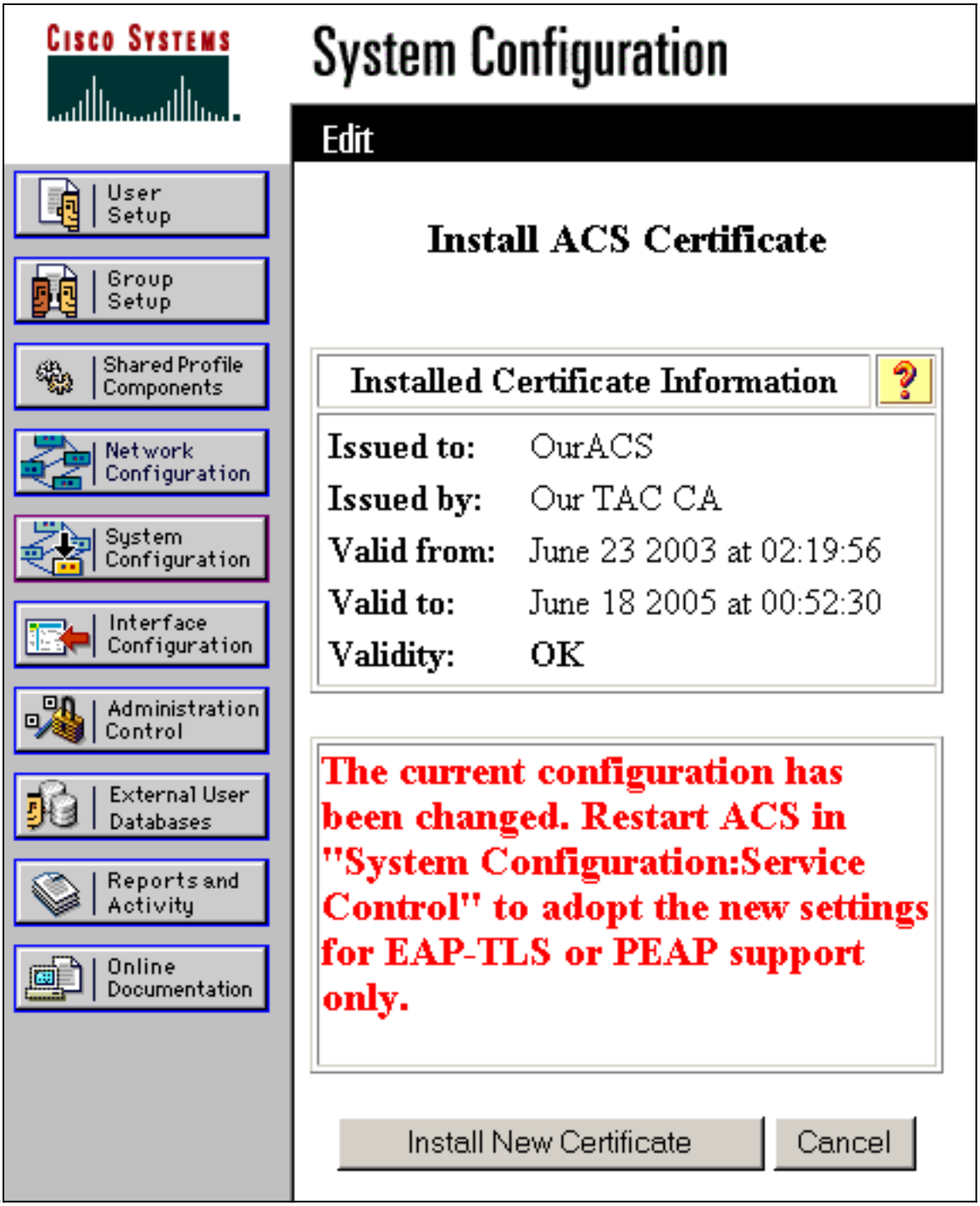
Suivez ces étapes pour configurer ACS pour utiliser le certificat dans la mémoire.

1. Ouvrez un navigateur Web et parcourez au serveur ACS en entrant dans **http:// *ACS-ip-address:2002/*** dans la barre d'adresses. Cliquez sur la **configuration système**, et puis cliquez sur l'**installation de certificat ACS**.
2. Le clic **installent le certificat ACS**.
3. **Certificat** choisi d'**utilisation de mémoire**. Dans le domaine NC de certificat, écrivez le nom du

certificat que vous avez assigné dans l'étape 5a de la section [obtenez un certificat pour le serveur ACS](). Cliquez sur **Submit**.Cette entrée doit apparier le nom que vous avez tapé dans la zone d'identification pendant la demande avancée de certificat. C'est le nom NC dans le domaine du certificat de serveur ; vous pouvez éditer le certificat de serveur pour vérifier ce nom. Dans cet exemple, le nom est « OurACS ». N'écrivez pas le nom NC de l'émetteur.



4. Quand la configuration est complète, vous verrez un message de confirmation indiquer que la configuration du serveur ACS a été changée.**Remarque:** Vous n'avez pas besoin de redémarrer l'ACS à ce

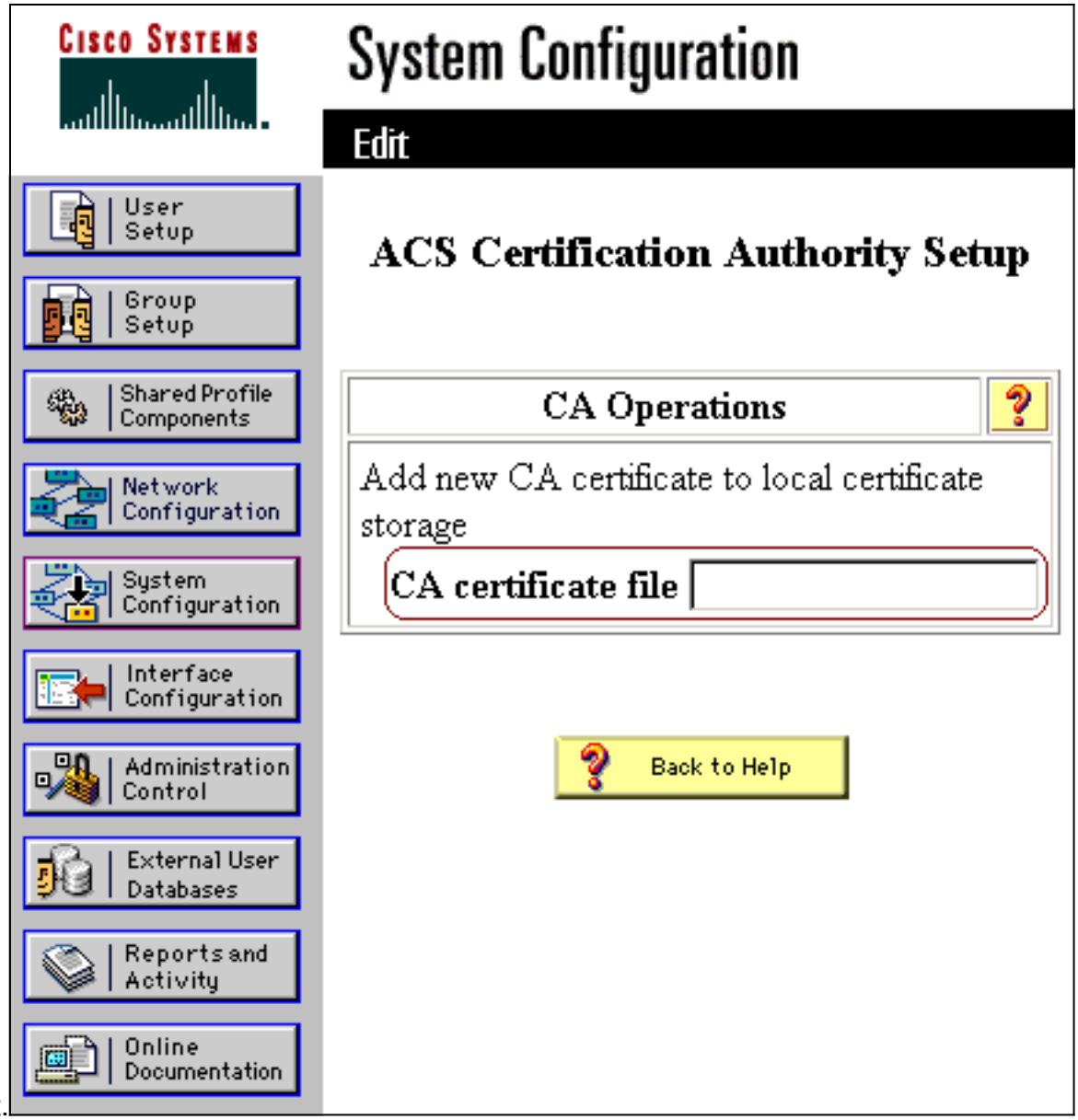


moment.

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

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

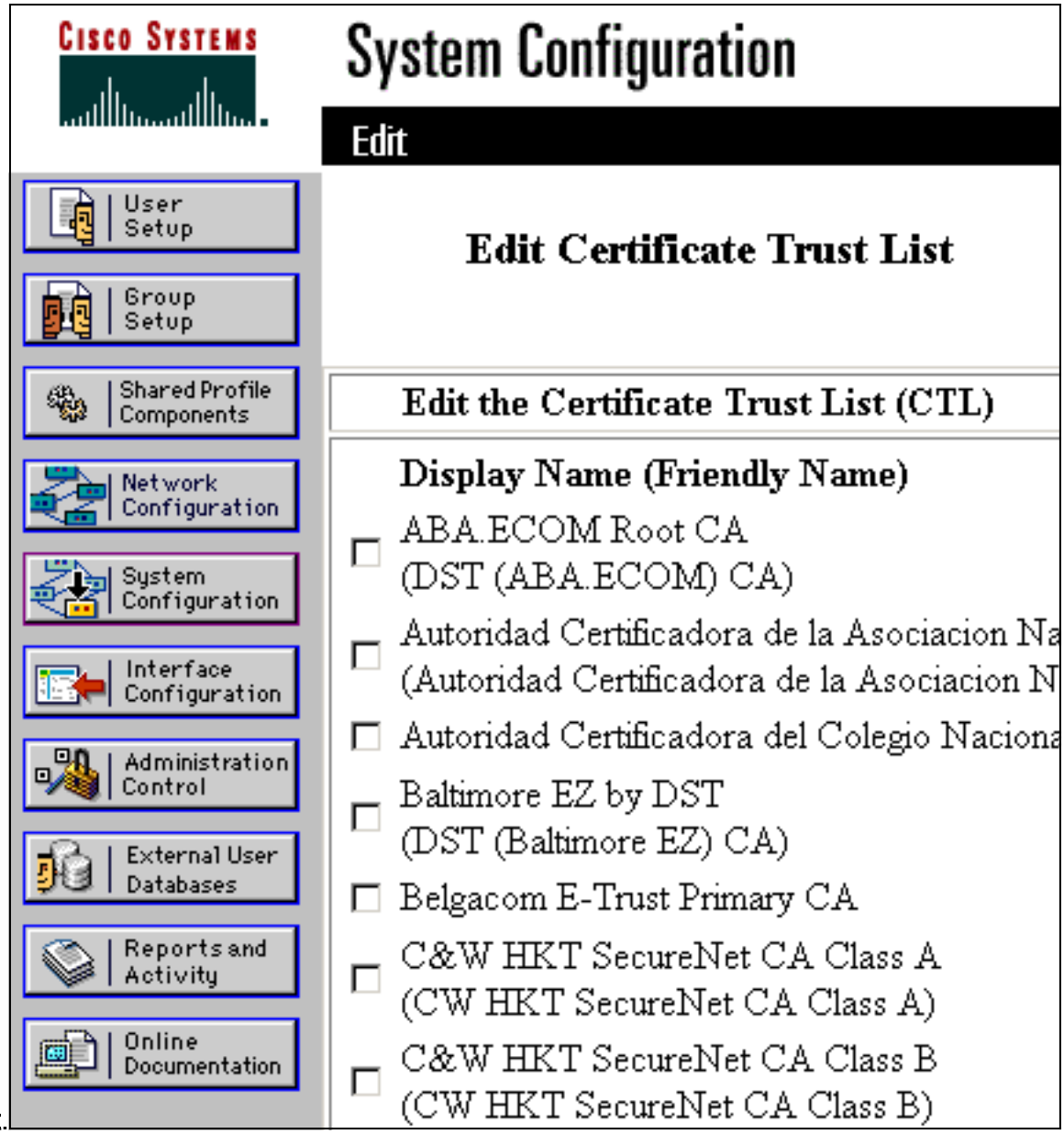
1. Cliquez sur la **configuration système**, et puis cliquez sur l'**installation de certificat ACS**.
2. Cliquez sur l'**installation d'autorité de certification ACS** pour ajouter le CAs à la liste de Certificats de confiance. Dans le domaine pour le fichier de certificat de CA, entrez l'emplacement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



Submit.

3. Cliquez sur Edit la **liste de confiance de certificat**. 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. Cliquez sur

Submit.



Redémarrez le service et configurez les configurations PEAP sur l'ACS

Suivez ces étapes pour redémarrer le service et pour configurer des configurations PEAP.

1. **La configuration système de** clic, et cliquent sur alors le **contrôle des services**.
2. **Reprise de** clic pour redémarrer le service.
3. Pour configurer des configurations PEAP, la **configuration système de** clic, et puis cliquer sur l'**installation globale d'authentification**.
4. Vérifiez les deux configurations affichées ci-dessous, et laissez toutes autres configurations en tant que par défaut. Si vous souhaitez, vous pouvez spécifier les configurations supplémentaires, telles qu'Enable Fast Reconnect. Quand vous êtes de finition, cliquez sur Submit.**Permettez EAP-MSCHAPv2Permettez l'authentification de version 2 MS-CHAPRemarque:** Pour plus d'informations sur rapide connectez, référez-vous « aux options de configuration d'authentification » en configuration système : Authentification et Certificats.