Secure ACS voor Windows v3.2 met EAP-TLS-machinverificatie

Inhoud

Inleiding

Dit document beschrijft hoe u de EXTRA COMPUTER-beveiliging (EAP-TLS) voor verificatie kunt configureren met Cisco Secure Access Control System (ACS) voor Windows versie 3.2.

Opmerking: Machineechtheidscontrole wordt niet ondersteund door de autoriteit voor het Novell-certificaat (CA). ACS kan EAP-TLS gebruiken om machine-verificatie te ondersteunen in Microsoft Windows Active Directory. De eindgebruiker client kan het protocol voor gebruikersverificatie beperken tot hetzelfde protocol dat wordt gebruikt voor de verificatie van machines. Voor het gebruik van EAP-TLS voor de authenticatie van de machine zou het gebruik van EAP-TLS's voor gebruikersauthenticatie nodig kunnen zijn. Raadpleeg het gedeelte Machineverificatie van de *Gebruikershandleiding voor Cisco Secure Access Control Server 4.1* voor meer informatie over

machineverantwoording.

Opmerking: Bij het opzetten van ACS om machines via EAP-TLS te authenticeren en het ACS is ingesteld voor Machineverificatie, moet de klant zodanig zijn ingericht dat hij alleen machineverantwoording doet. Raadpleeg voor meer informatie Hoe u alleen-computerverificatie kunt inschakelen voor een op 802.1X gebaseerd netwerk in Windows Vista, in Windows Server 2008 en in Windows XP Service Pack 3.

Voorwaarden

Vereisten

Er zijn geen specifieke voorwaarden van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de onderstaande software- en hardwareversies.

- Cisco Secure ACS voor Windows versie 3.2
- Microsoft certificaatservices (geïnstalleerd als autoriteit voor Enterprise root [CA])**Opmerking:** Raadpleeg voor meer informatie de stapsgewijze gids voor het instellen van een certificeringsinstantie .
- DNS-service met Windows 2000-server met servicepack 3 en hotfix 323172**Opmerking:** Als u CA Server-problemen ondervindt, installeert u hotfix 323172 . De Windows 2000 SP3-client vereist hotfix 313664 om IEEE 802.1x-verificatie in te schakelen.
- Cisco Aironet 1200 Series draadloos access point 12.01T
- IBM ThinkPad T30 met Windows XP Professional met Service Pack 1

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Achtergrondinformatie

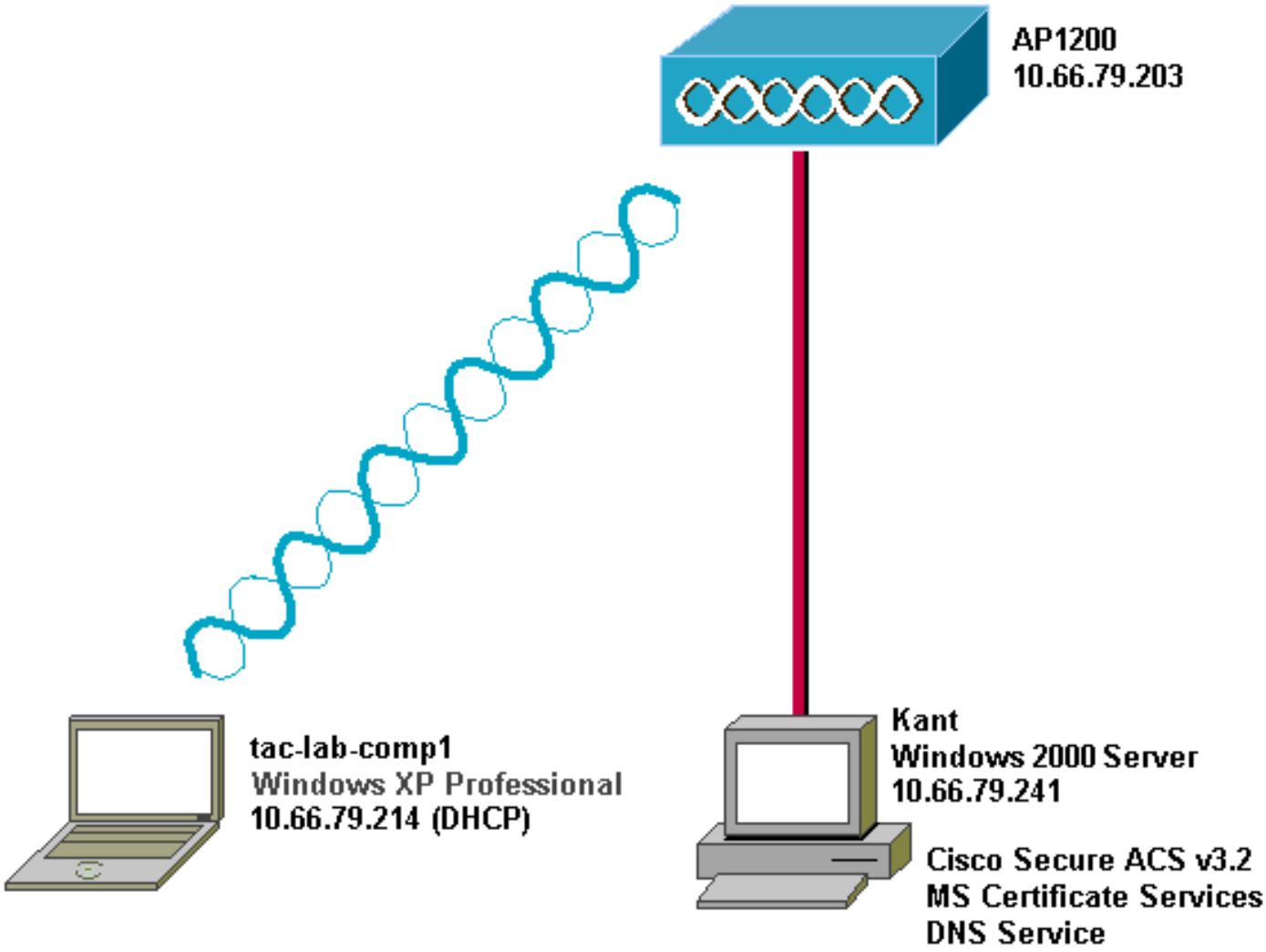
Zowel EAP-TLS als Protected Extensible Authentication Protocol (PEAP) bouwen en gebruiken een TLS/Secure Socket Layer (SSL)-tunnel. EAP-TLS maakt gebruik van wederzijdse authenticatie waarbij zowel de ACS-server (authenticatie, autorisatie en accounting [AAA]) als de klanten over certificaten beschikken en hun identiteit aan elkaar bewijzen. PEAP gebruikt echter alleen authenticatie aan serverzijde; alleen de server heeft een certificaat en bewijst zijn identiteit aan de cliënt .

Conventies

Zie de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in het onderstaande schema zijn weergegeven.



Cisco Secure ACS voor Windows v3.2 configureren

Volg de onderstaande stappen om ACS 3.2 te configureren.

1. Verkrijg een certificaat voor de ACS server.
2. ACS configureren om een opslagcertificaat te gebruiken.
3. Specificeer aanvullende certificeringsinstanties die de ACS moeten vertrouwen.
4. Start de service opnieuw en stel PEAP-instellingen in op de ACS.
5. Specificeer en configureren het access point als een AAA-client.
6. Het configureren van de externe gebruikersdatabases.
7. Start de service opnieuw.

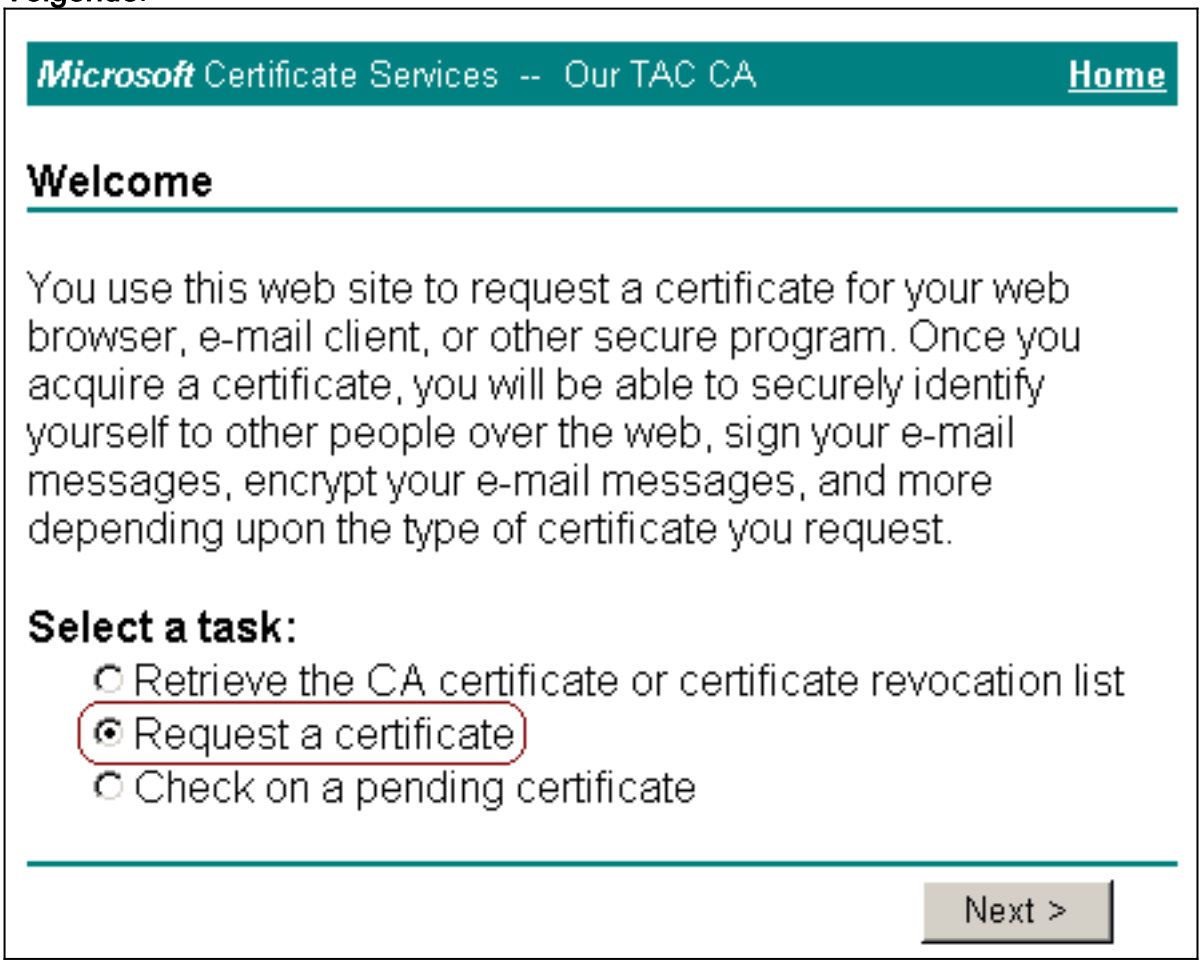
Een certificaat voor de ACS-server verkrijgen

Volg deze stappen om een certificaat te verkrijgen.

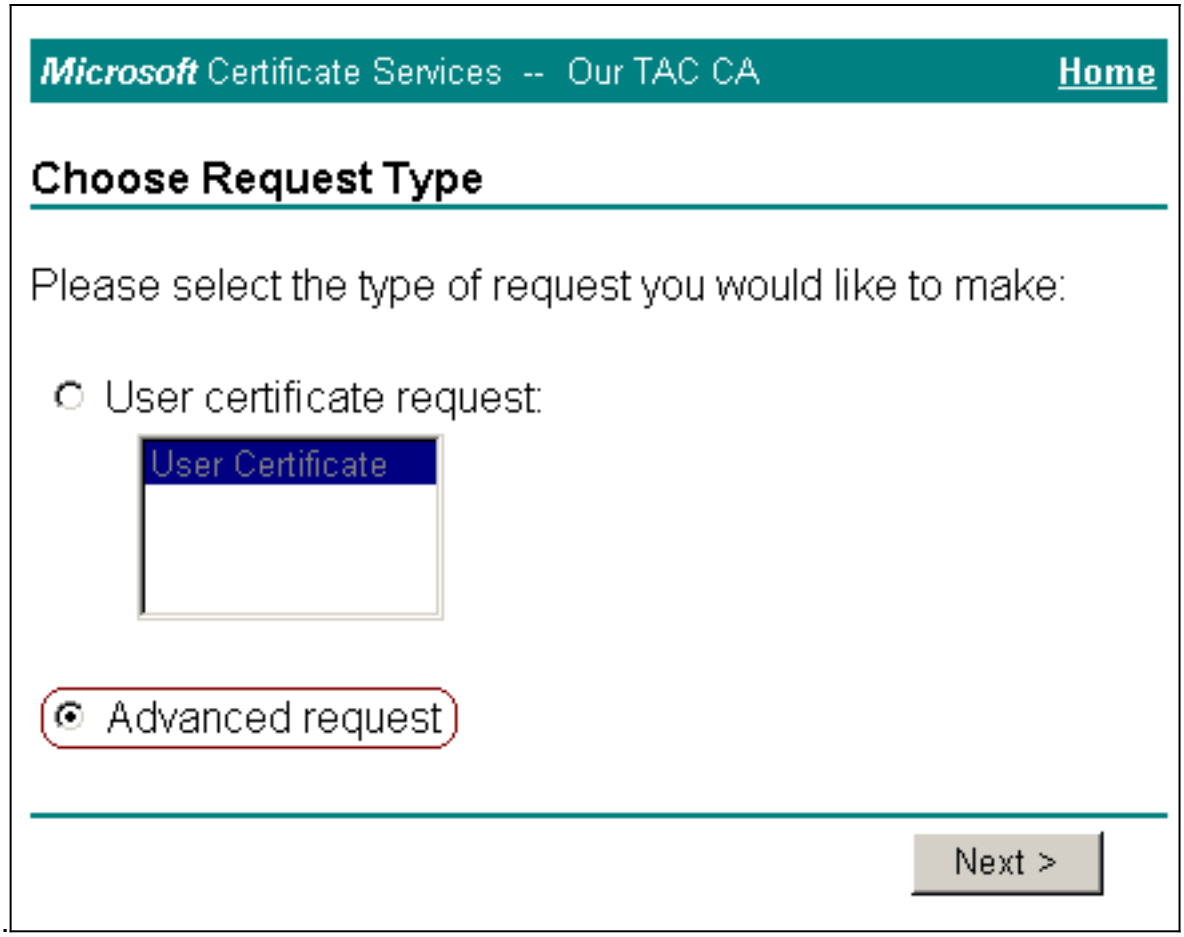
1. Open op de ACS-server een webbrowser en voer **http:// *CA-ip-adres*/certsrv in** om toegang te krijgen tot de CA-server.
2. Meld u aan bij het domein als

beheerder.

3. Selecteer **Een certificaat aanvragen** en klik vervolgens op **Volgende**.

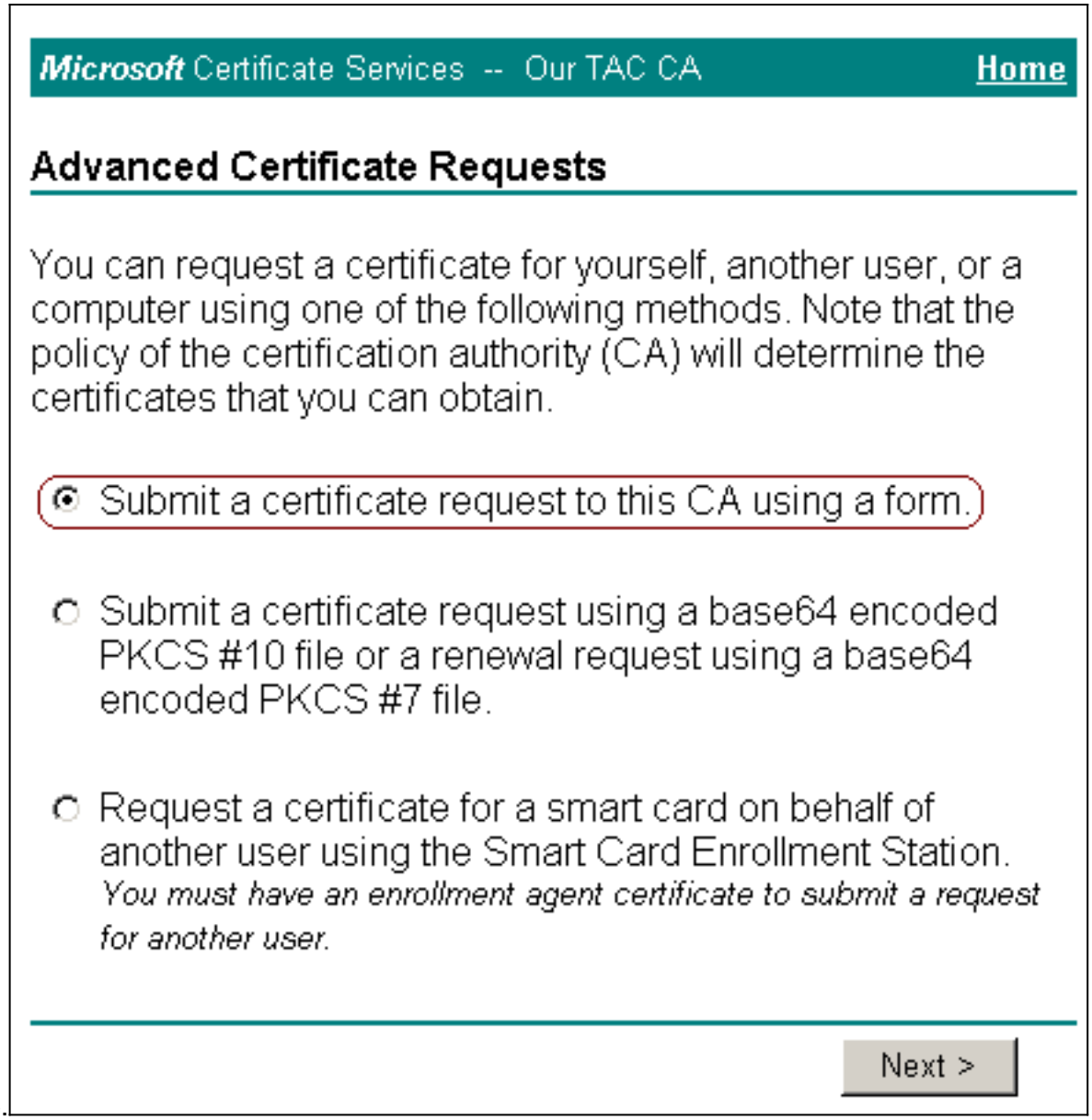


4. Selecteer **Geavanceerd verzoek** en klik vervolgens op



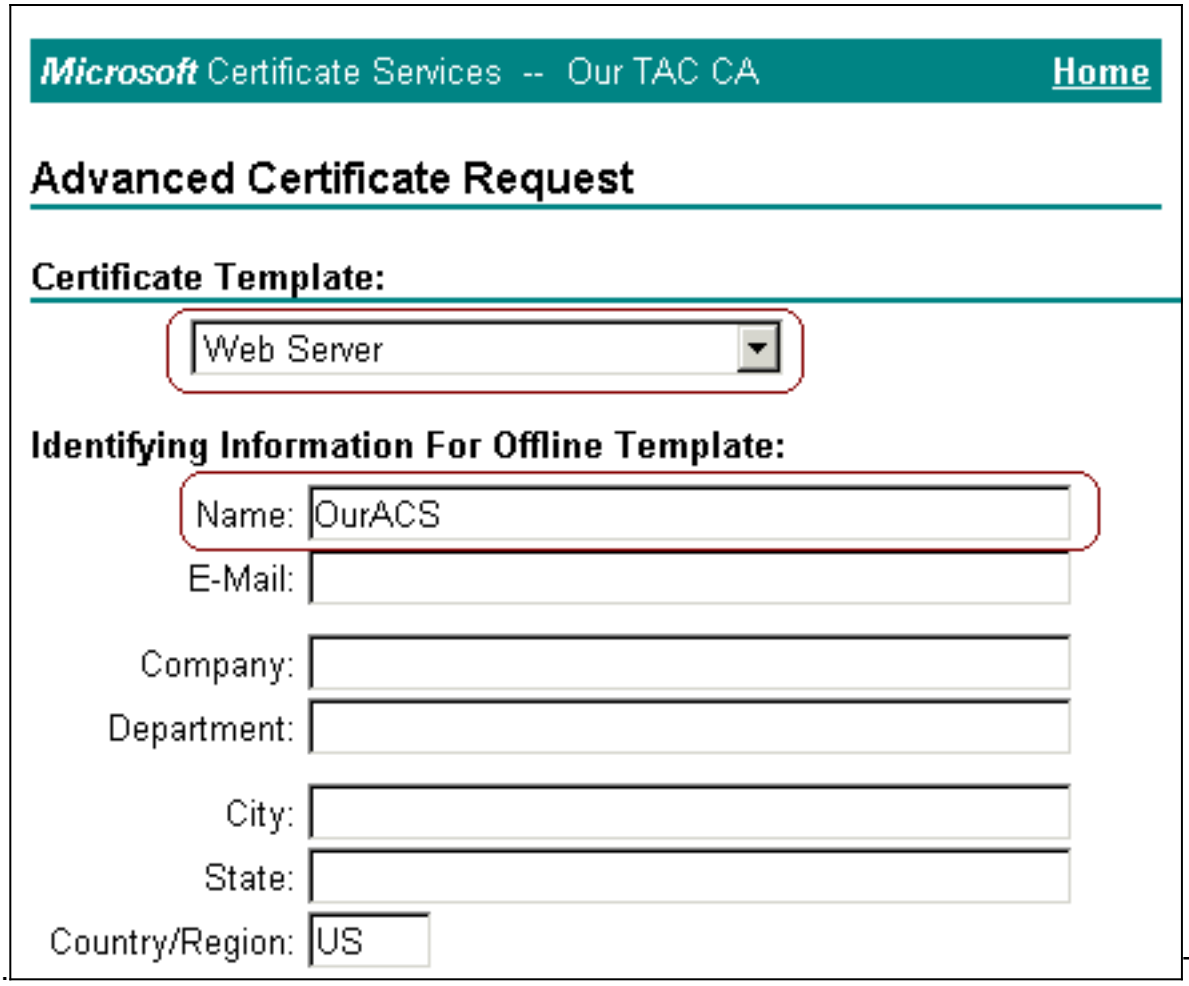
Volgende.

5. Selecteer **een certificaataanvraag bij deze CA indienen met behulp van een formulier** en klik vervolgens op

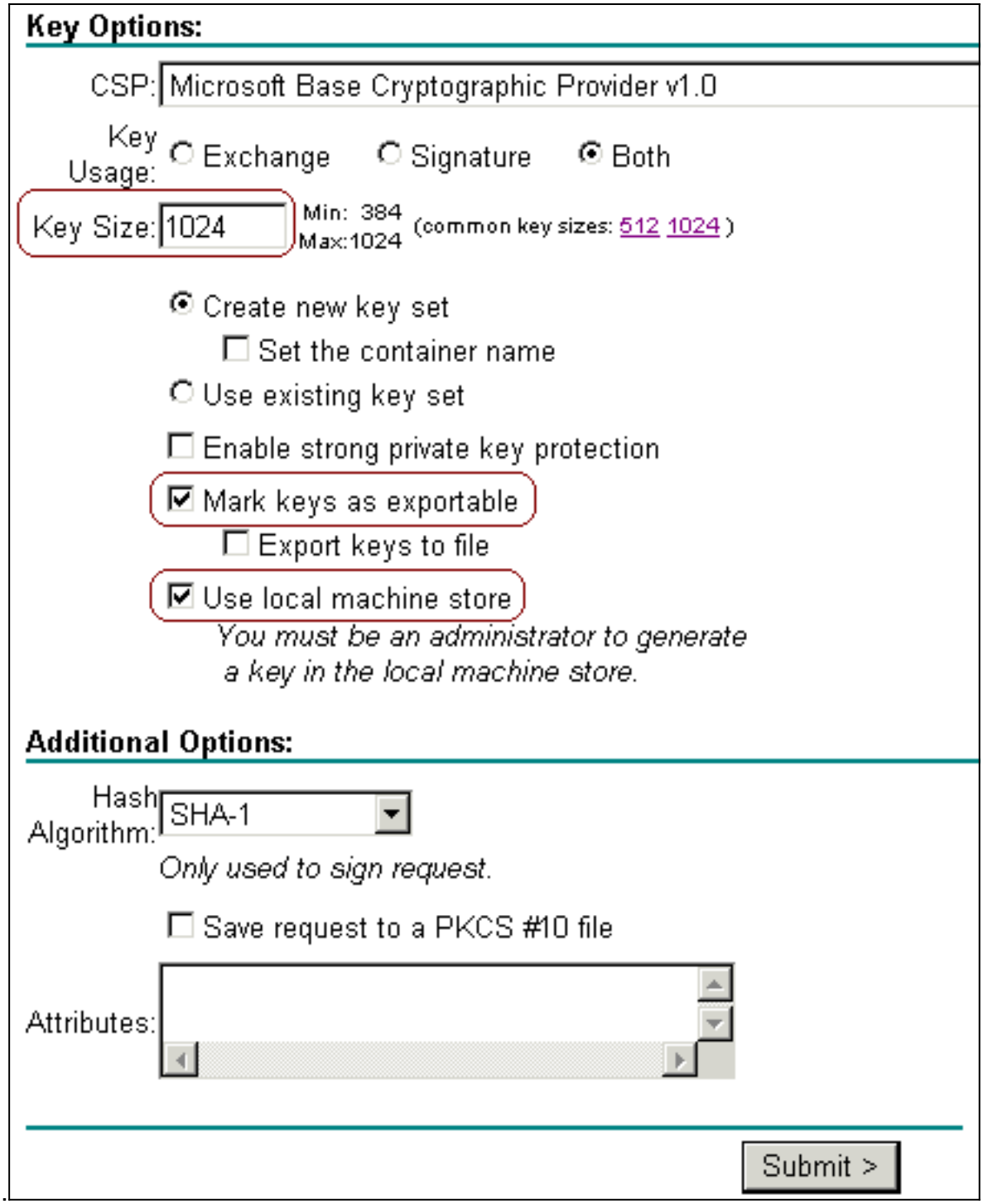


Volgende.

6. Configuratie van de certificeringsopties:Selecteer **Webserver** als de certificaatsjabloon en voer de naam van de ACS-server



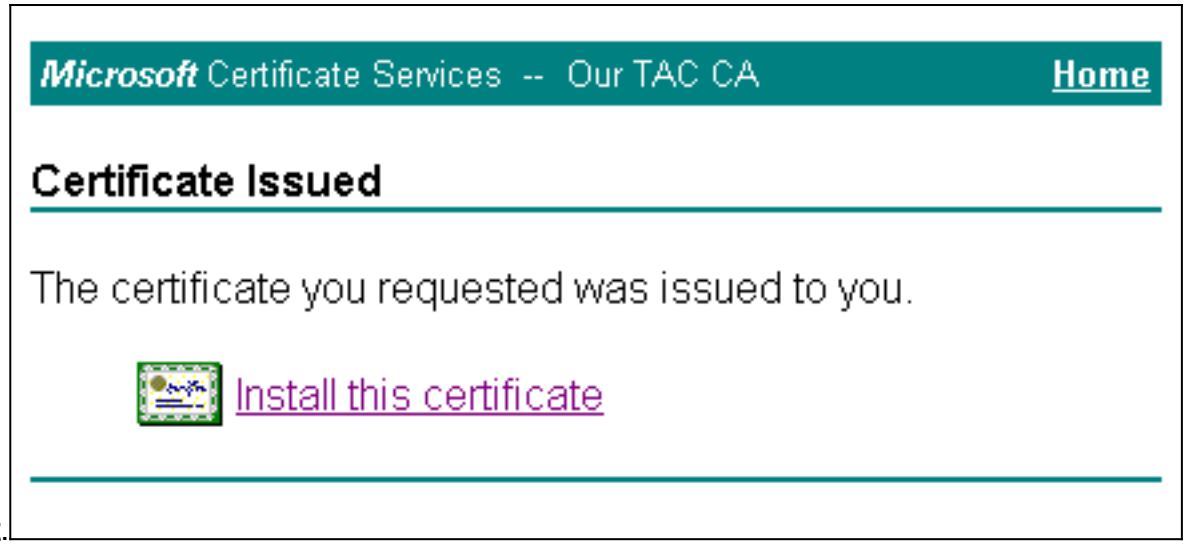
in. Typ **1024** in het veld Key Size en controleer de **Mark-toetsen als exportbaar** en **gebruik de** vinkjes **van de lokale machinewinkel**.Configureer de gewenste opties en klik vervolgens op



Indienen.

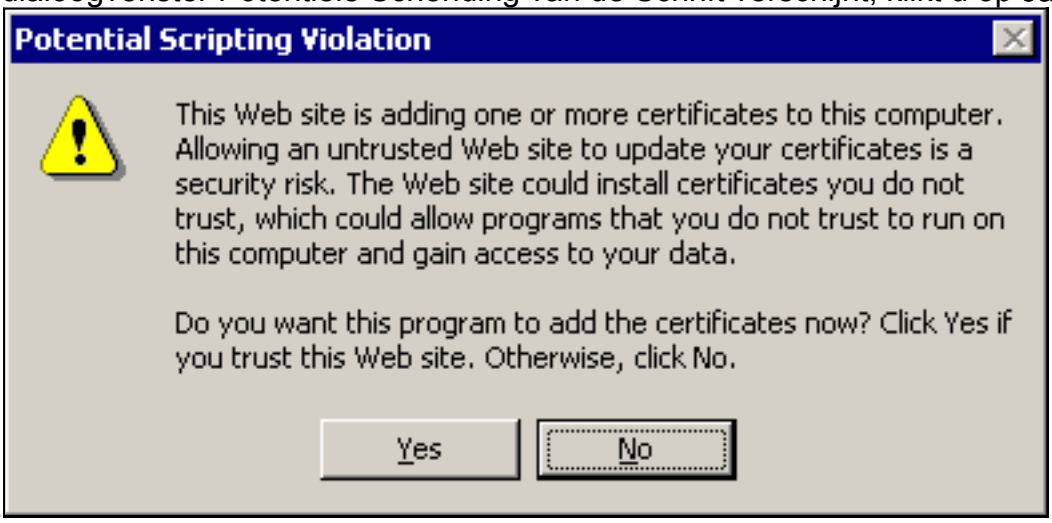
N.B.: Als het dialoogvenster Potentiële Schending van de Schrift verschijnt, klikt u op **Ja** om door te gaan.

7. Klik op **Installeer dit**

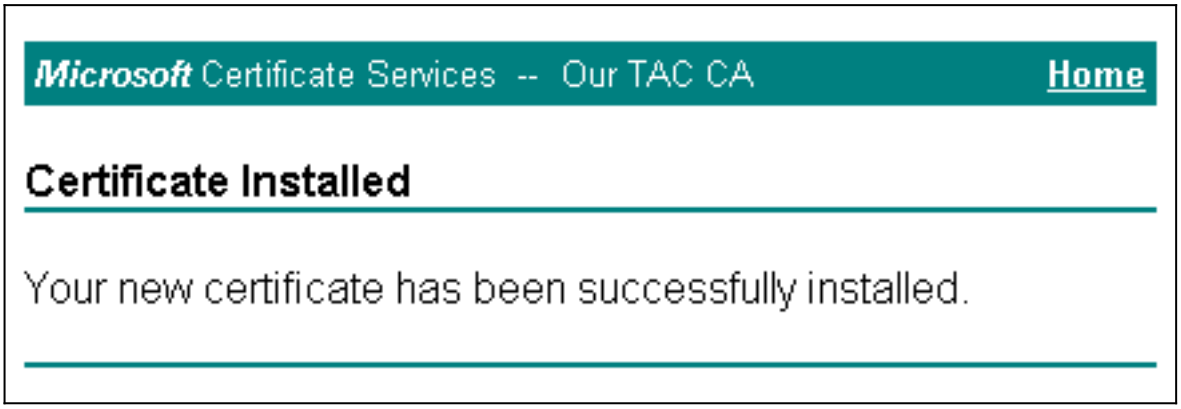


certificaat.

N.B.: Als het dialoogvenster Potentiële Schending van de Schrift verschijnt, klikt u op **Ja** om door te gaan.



8. Als de installatie geslaagd is, verschijnt het geïnstalleerde bericht van het Certificaat.



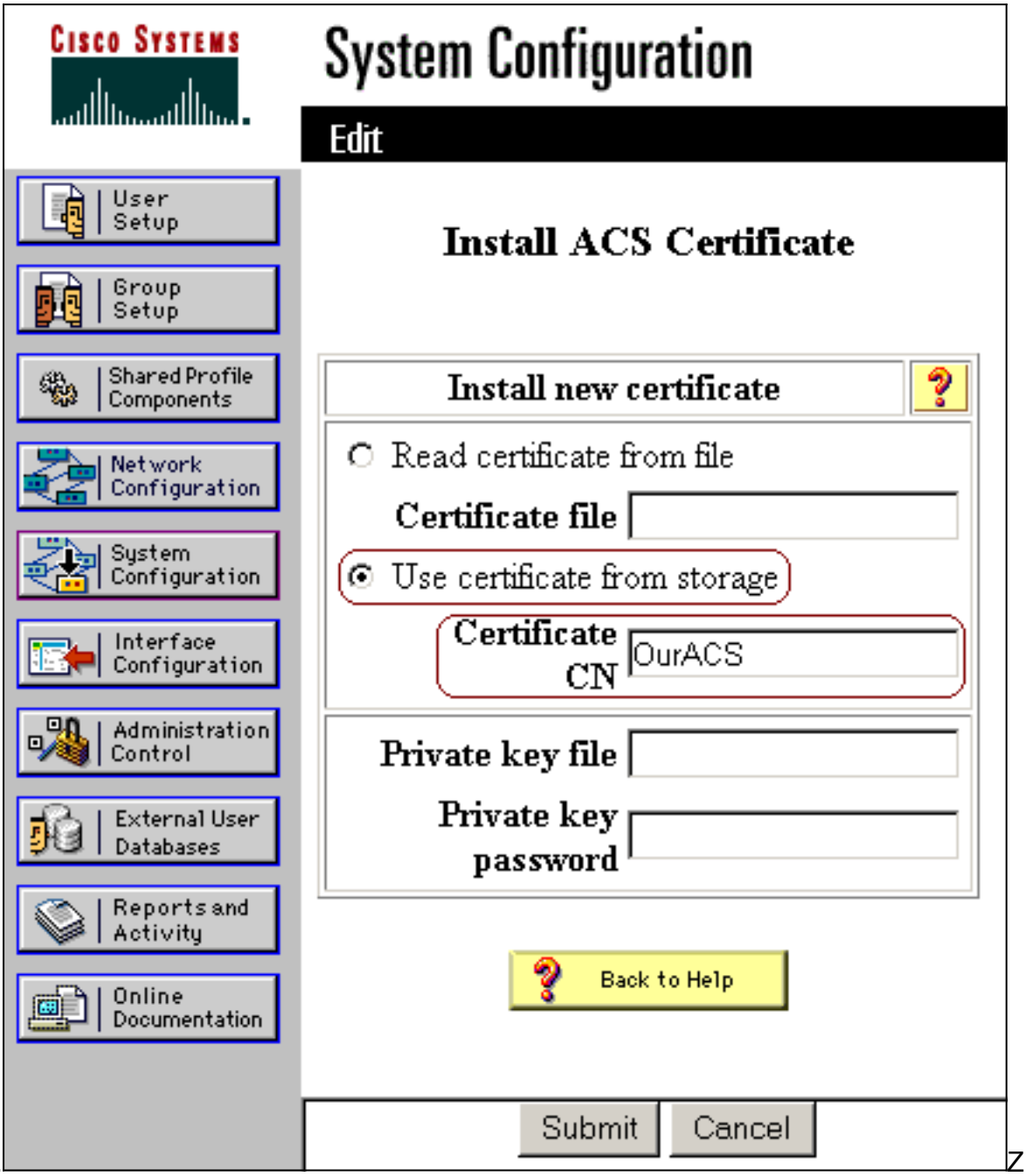
ACS configureren voor gebruik van een opslagcertificaat

Voltooi deze stappen om ACS te configureren om het opgeslagen certificaat te gebruiken.

1. Open een webbrowser en voer **http:// *ACS-ip-adres in*:2002/**om toegang te krijgen tot de ACS-server.
2. Klik op **System Configuration** en vervolgens op **ACS-certificaatinstelling**.
3. Klik op **ACS-certificaat installeren**.
4. Klik **vanuit het** keuzerondje **Storage op het certificaat**.
5. Voer in het veld certificaatGN de naam in van het certificaat dat u in stap 5a van het vak

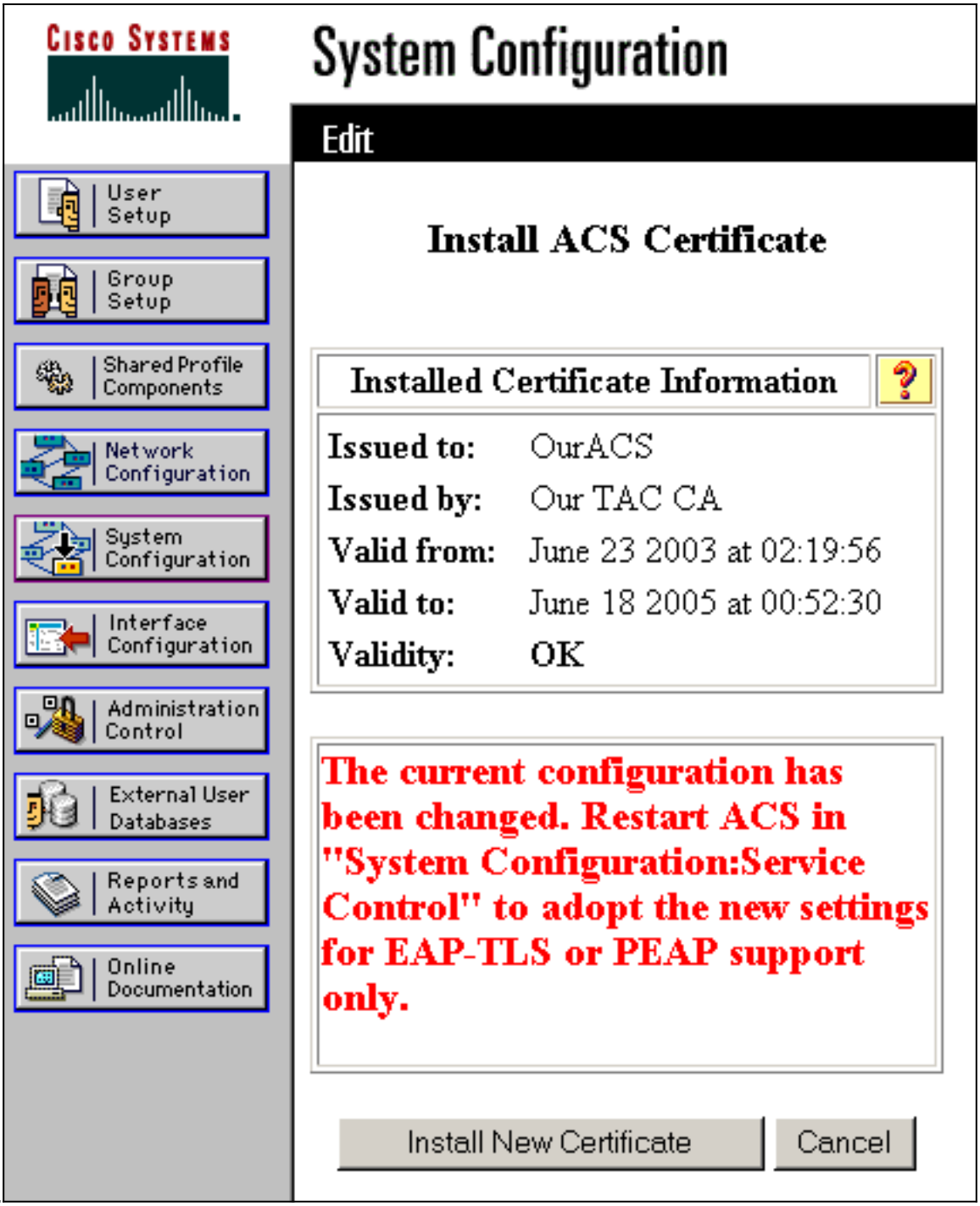
Certificaat verkrijgen van de ACS-server van dit document hebt toegewezen.

6. Klik op



Inzenden. Zodra de configuratie is voltooid, verschijnt er een bevestigingsbericht dat aangeeft dat de configuratie van de ACS-server is gewijzigd.**Opmerking:** U hoeft het ACS-systeem op dit moment niet opnieuw te

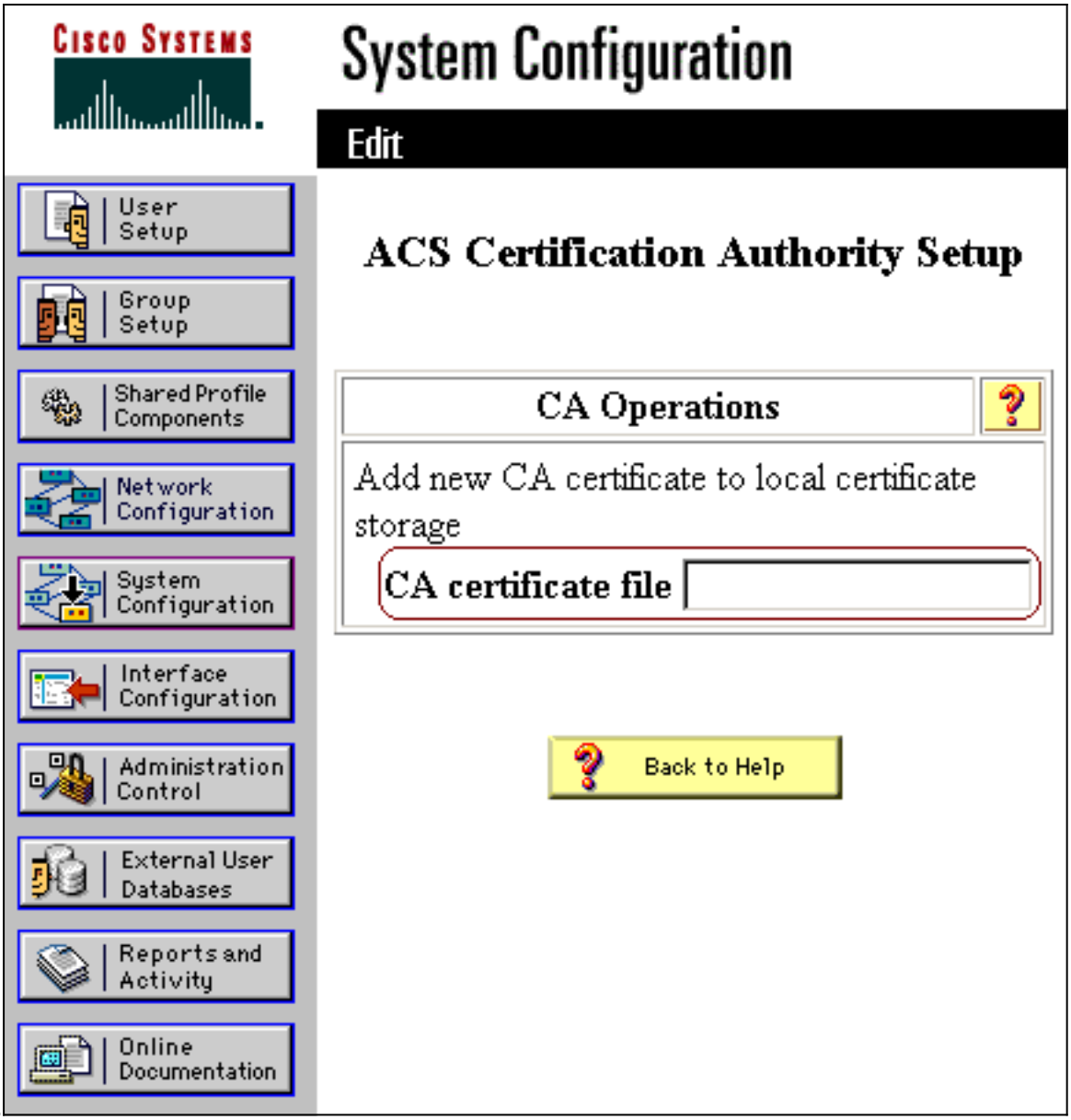
starten.



Specificeer aanvullende certificeringsinstanties die de ACS moeten vertrouwen

ACS vertrouwt automatisch op de CA die haar eigen certificaat heeft afgegeven. Als de client-certificaten zijn afgegeven door extra CA's, moet u deze stappen voltooien:

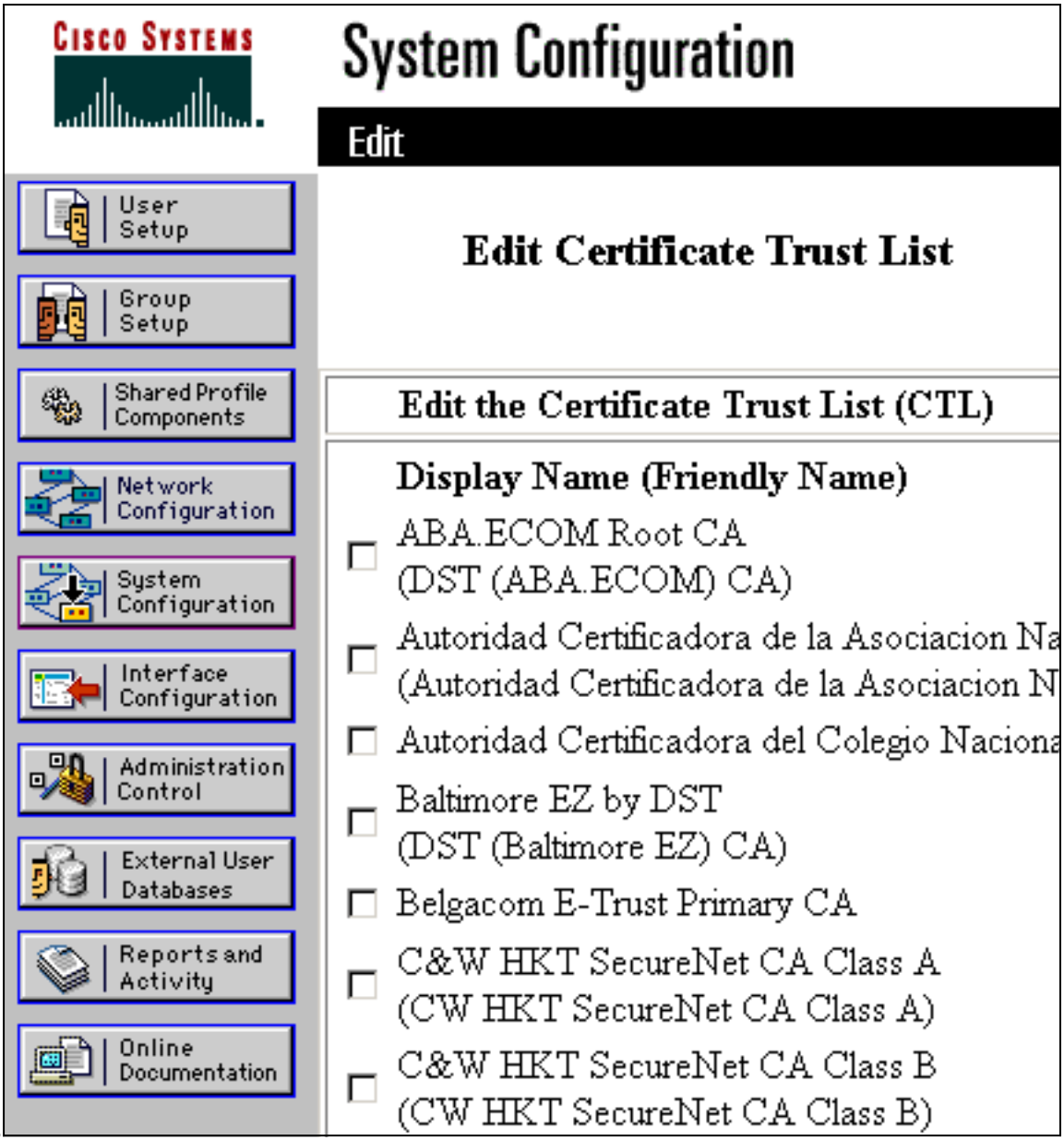
1. Klik op **System Configuration** en vervolgens op **ACS-certificaatinstelling**.
2. Klik op **ACS certificaatinstelling** om CA's aan de lijst van vertrouwde certificaten toe te voegen.
3. Typ in het veld voor CA-certificaatbestand de locatie van het certificaat en klik vervolgens op



Inzenden.

4. Klik op **certificaatlijst bewerken**.
5. Controleer alle CA's die de ACS moeten vertrouwen en verwijder alle CA's die de ACS niet moeten vertrouwen.
6. Klik op

Inzenden.



Start de service opnieuw en stel de EAP-TLS-instellingen in op de ACS

Voltooi deze stappen om de service te hervatten en stel de instellingen van EAP-TLS in:

1. Klik op **System Configuration** en vervolgens op **Service Control**.
2. Klik op **Start** opnieuw om de service te hervatten.
3. Klik om de instellingen van EAP-TLS te configureren op **System Configuration** en klik vervolgens op **Global Authentication Setup**.
4. Controleer **MAP-TLS toestaan** en controleer vervolgens een of meer van de certificaatvergelijkingen.
5. Klik op