Sicherer ACS für Windows v3.2 mit EAP-TLS-Computerauthentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) mit dem Cisco Secure Access Control System (ACS) für Windows 3.2 konfigurieren.

Hinweis: Die Maschinenauthentifizierung wird von der Novell Certificate Authority (CA) nicht unterstützt. ACS kann EAP-TLS verwenden, um die Systemauthentifizierung für Microsoft Windows Active Directory zu unterstützen. Der Endbenutzer-Client kann das Protokoll für die Benutzerauthentifizierung auf dasselbe Protokoll beschränken, das für die Computerauthentifizierung verwendet wird. Das heißt, die Verwendung von EAP-TLS für die maschinelle Authentifizierung kann die Verwendung von EAP-TLS für die

Benutzerauthentifizierung erfordern. Weitere Informationen zur Computerauthentifizierung finden Sie im Abschnitt Computerauthentifizierung im *Benutzerhandbuch für Cisco Secure Access Control Server 4.1*.

Hinweis: Wenn der ACS für die Authentifizierung von Computern über EAP-TLS eingerichtet wurde und der ACS für die maschinelle Authentifizierung eingerichtet wurde, muss der Client so konfiguriert werden, dass er nur die maschinelle Authentifizierung durchführt. Weitere Informationen finden Sie unter Aktivieren der Nur-Computer-Authentifizierung für ein 802.1X-basiertes Netzwerk in Windows Vista, Windows Server 2008 und Windows XP Service Pack 3.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco Secure ACS für Windows Version 3.2
- Microsoft Certificate Services (installiert als Enterprise Root Certificate Authority [CA])**Hinweis:** Weitere Informationen finden Sie im schrittweisen Handbuch zum Einrichten einer Zertifizierungsstelle .
- DNS-Dienst mit Windows 2000 Server mit Service Pack 3 und Hotfix 323172**Hinweis:** Wenn Probleme mit CA Server auftreten, installieren Sie Hotfix 323172 . Der Windows 2000 SP3 Client benötigt Hotfix 313664 , um die IEEE 802.1x-Authentifizierung zu aktivieren.
- Cisco Aironet 12.01T Wireless Access Point der Serie 1200
- IBM ThinkPad T30 mit Windows XP Professional und Service Pack 1

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Hintergrundtheorie

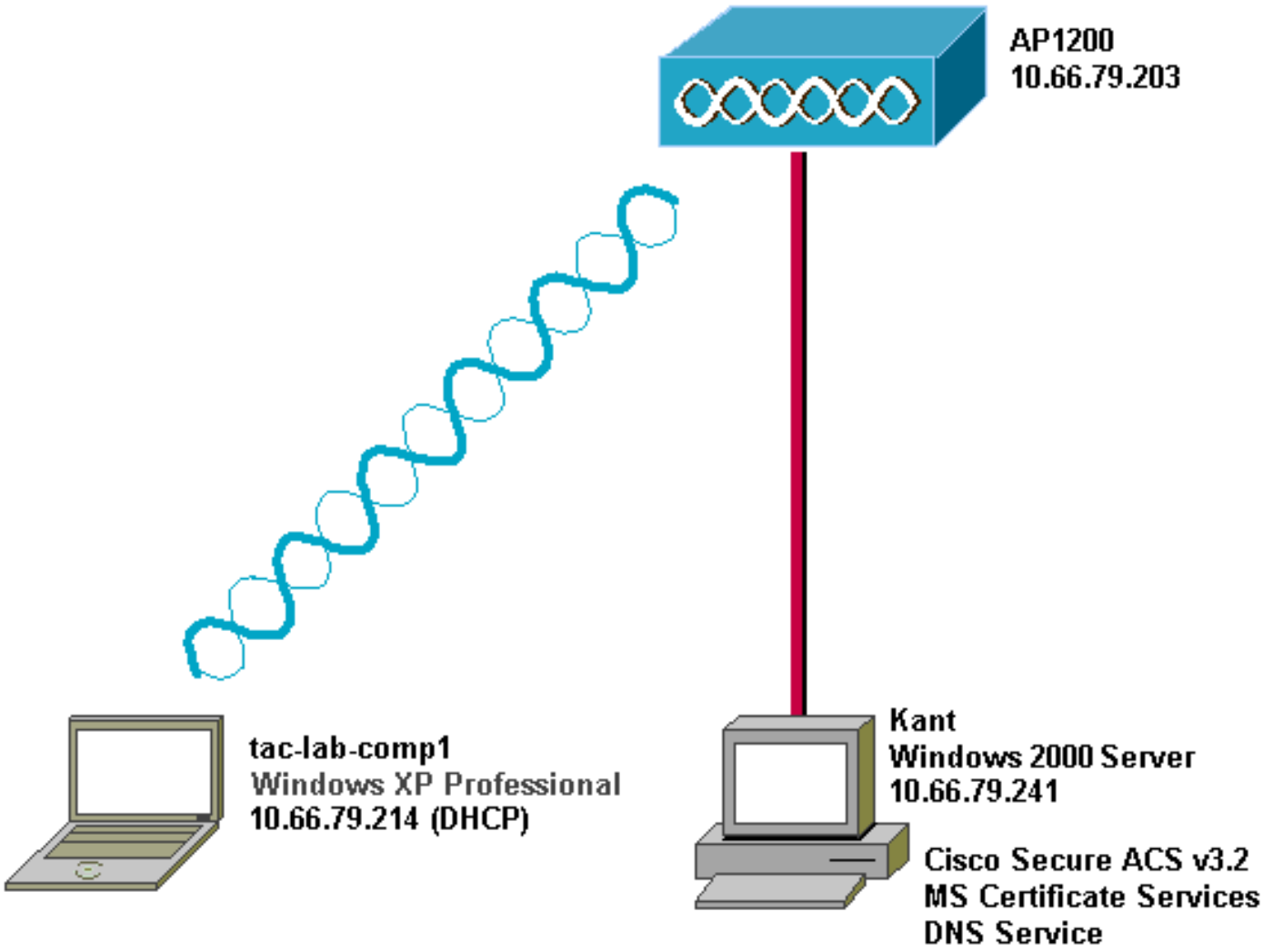
Sowohl EAP-TLS als auch Protected Extensible Authentication Protocol (PEAP) erstellen und verwenden einen TLS/Secure Socket Layer (SSL)-Tunnel. EAP-TLS verwendet gegenseitige Authentifizierung, bei der sowohl der ACS-Server (Authentication, Authorization, Accounting [AAA]) als auch die Clients Zertifikate besitzen und ihre Identitäten untereinander nachweisen. PEAP verwendet jedoch nur die serverseitige Authentifizierung. Nur der Server verfügt über ein Zertifikat und beweist seine Identität gegenüber dem Client.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Netzwerkdiagramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



Konfigurieren von Cisco Secure ACS für Windows 3.2

Folgen Sie den Schritten unten, um ACS 3.2 zu konfigurieren.

1. Erhalten Sie ein Zertifikat für den ACS-Server.
2. Konfigurieren des ACS zur Verwendung eines Zertifikats aus dem Speicher.
3. Geben Sie zusätzliche Zertifizierungsstellen an, denen der ACS vertrauen soll.
4. Starten Sie den Dienst neu, und konfigurieren Sie PEAP-Einstellungen auf dem ACS.
5. Angeben und Konfigurieren des Access Points als AAA-Client.
6. Konfigurieren Sie die externen Benutzerdatenbanken.
7. Starten Sie den Dienst neu.

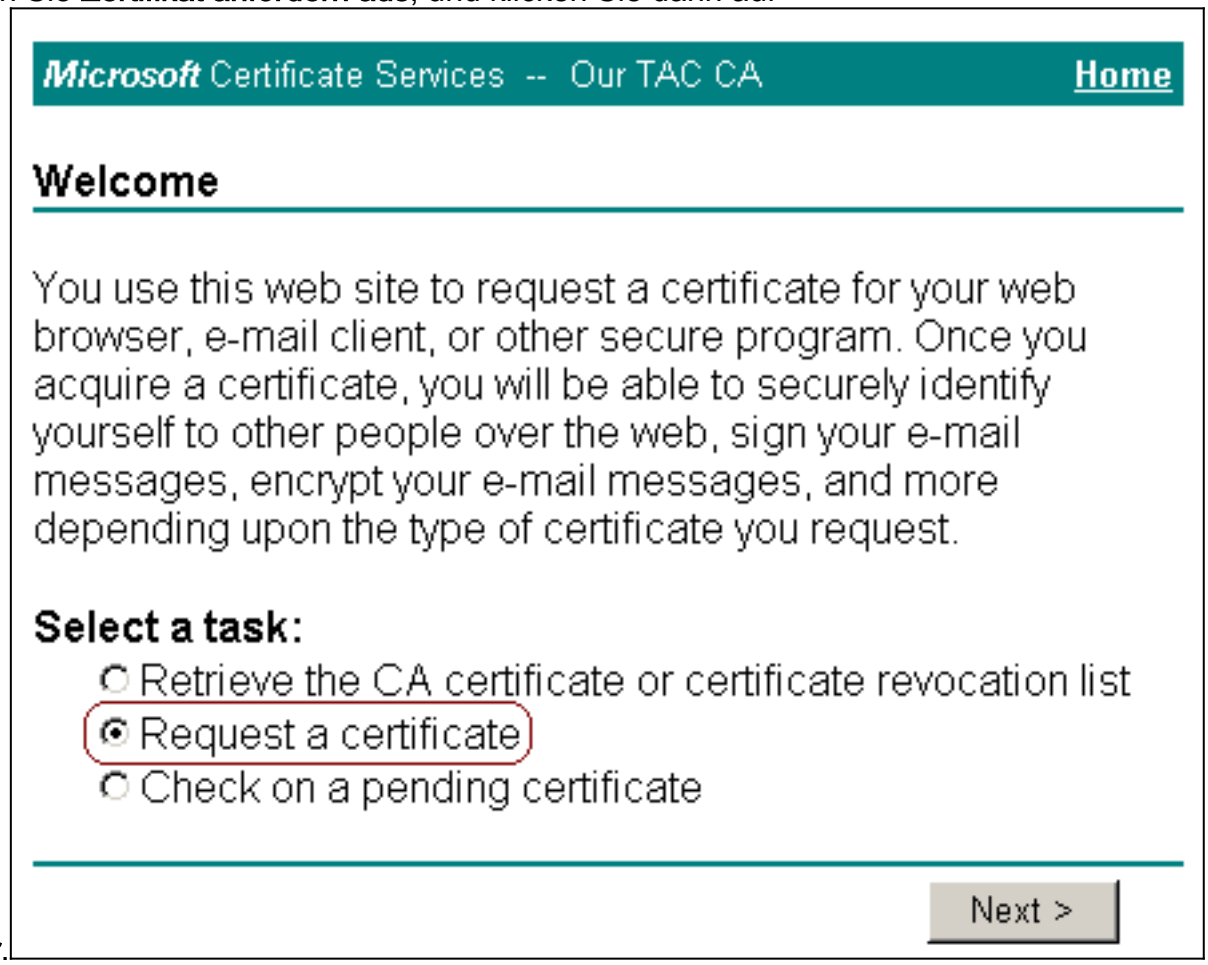
Zertifikat für den ACS-Server abrufen

Befolgen Sie diese Schritte, um ein Zertifikat zu erhalten.

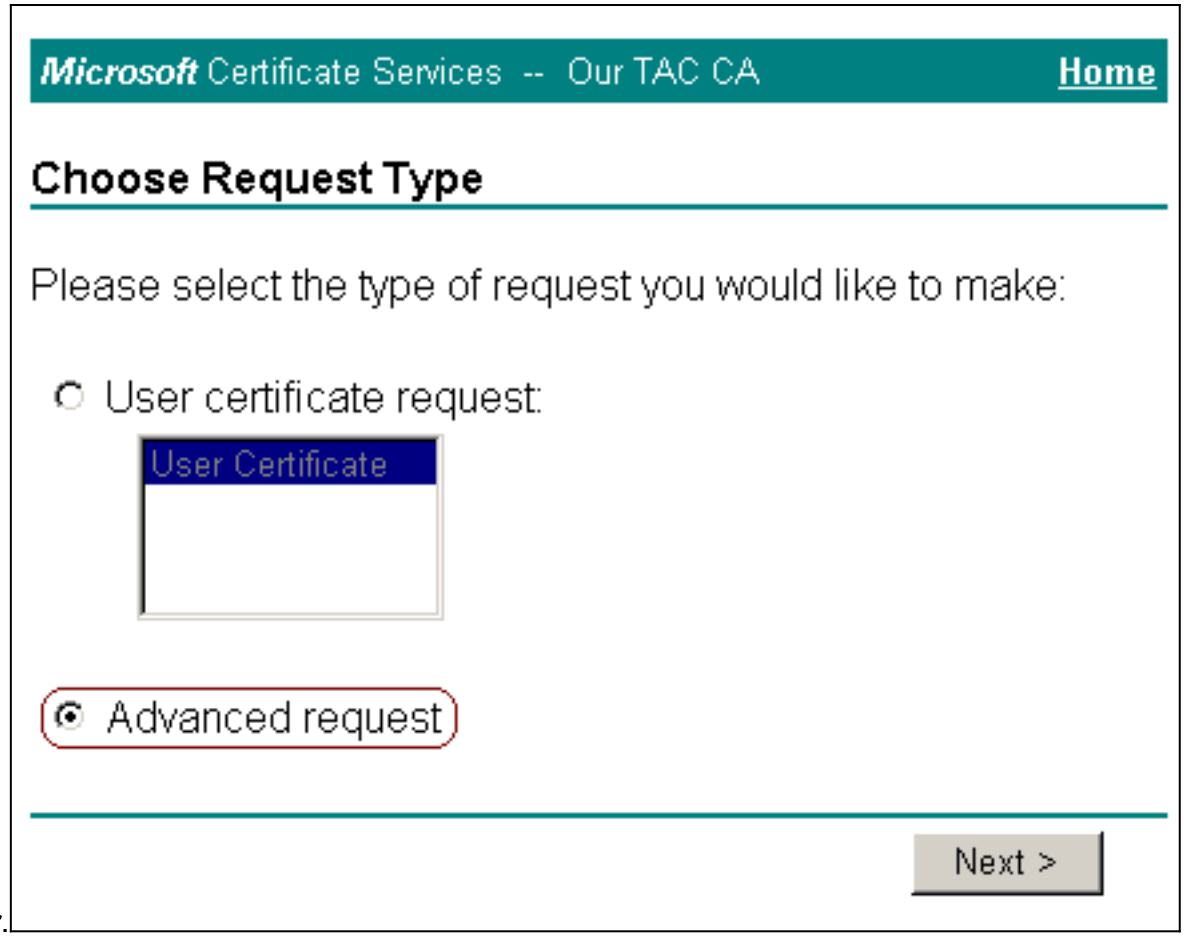
1. Öffnen Sie auf dem ACS-Server einen Webbrowser, und geben Sie **http://*CA-ip-address*/certsrv ein**, um auf den CA-Server zuzugreifen.

2. Melden Sie sich als Administrator bei der Domäne an.

3. Wählen Sie **Zertifikat anfordern aus**, und klicken Sie dann auf **Weiter**.

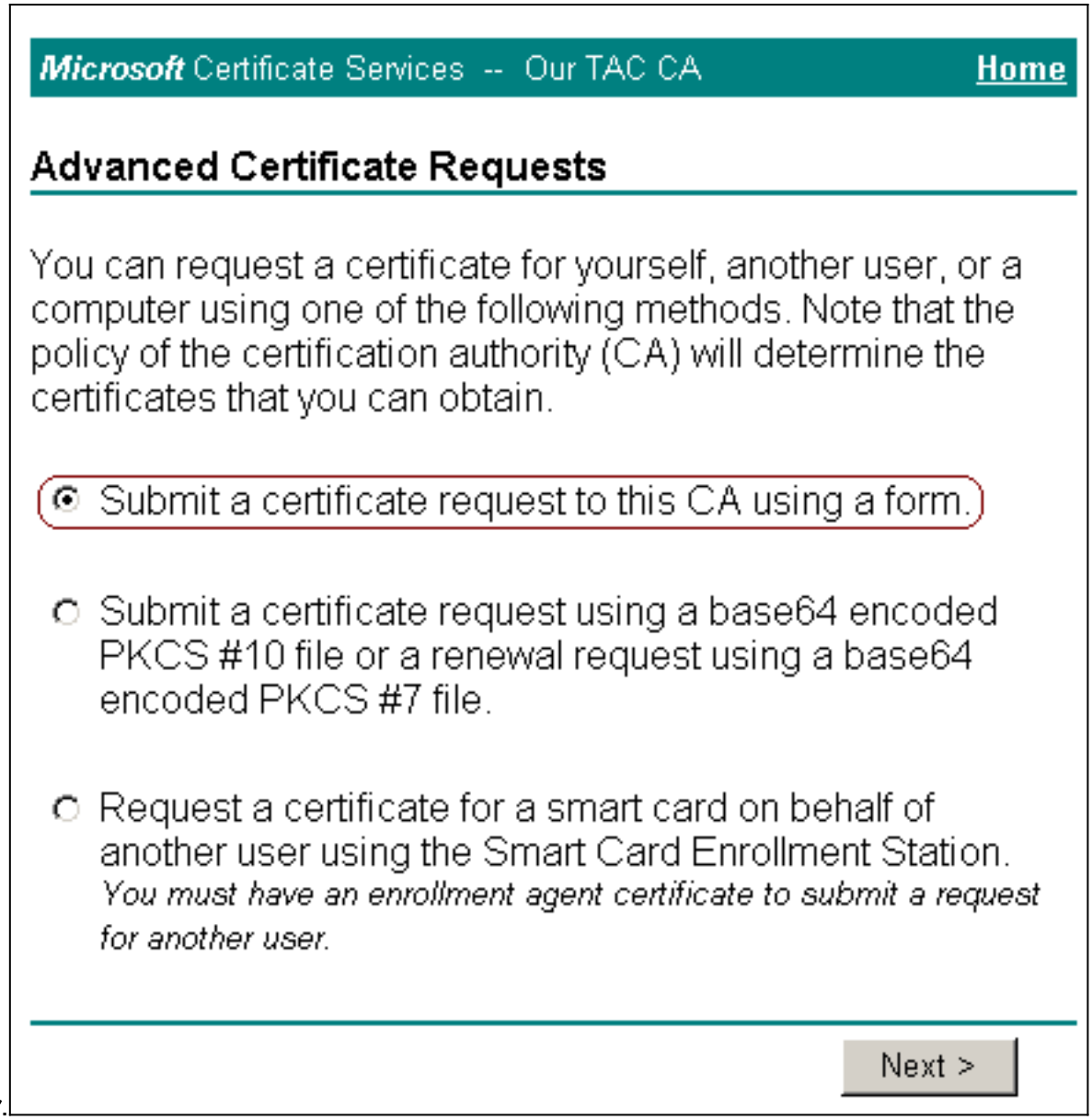


4. Wählen Sie **Erweiterte Anforderung aus**, und klicken Sie dann auf



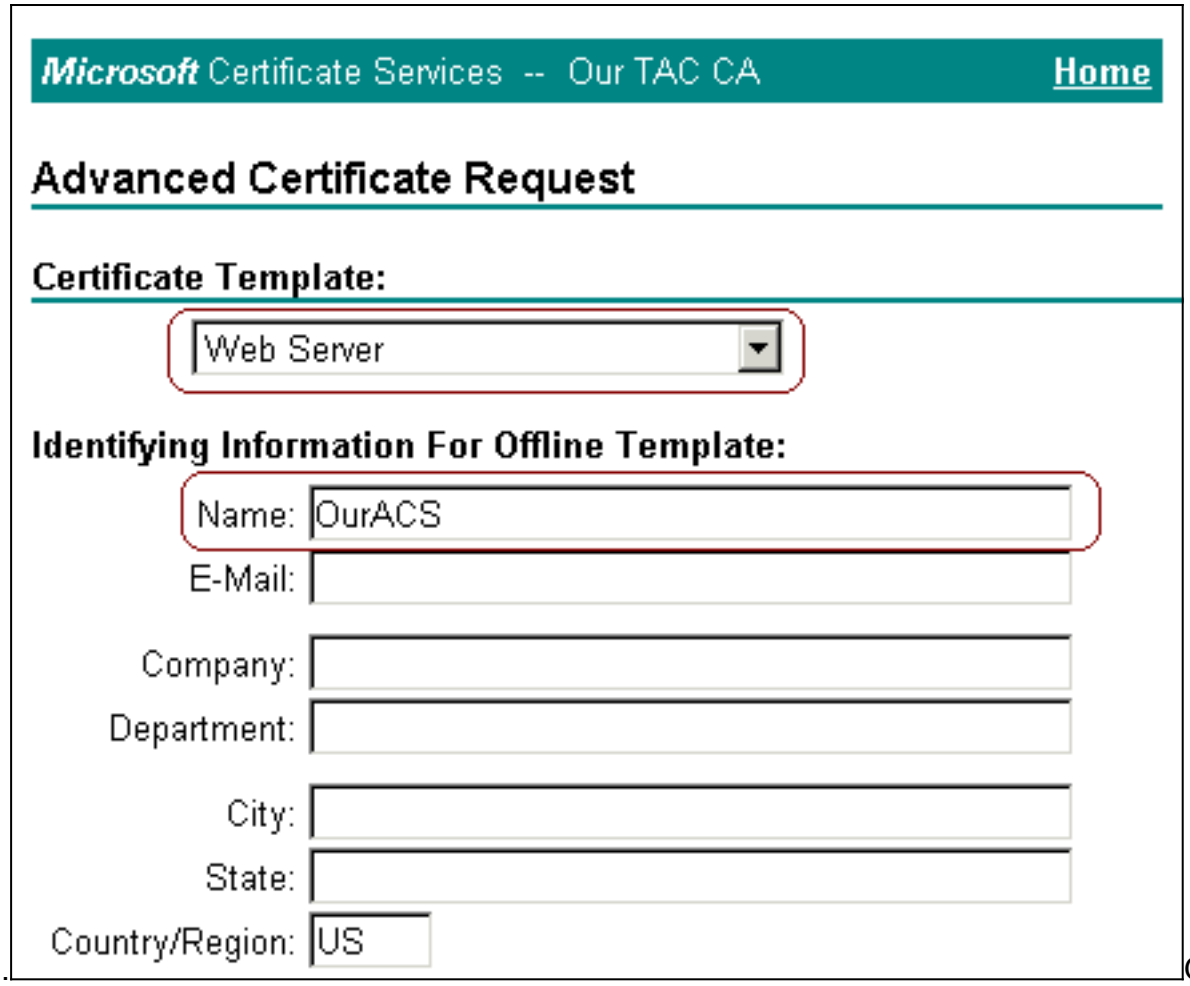
Weiter.

5. Wählen Sie **eine Zertifikatsanforderung an diese Zertifizierungsstelle mithilfe eines Formulars senden aus**, und klicken Sie dann auf

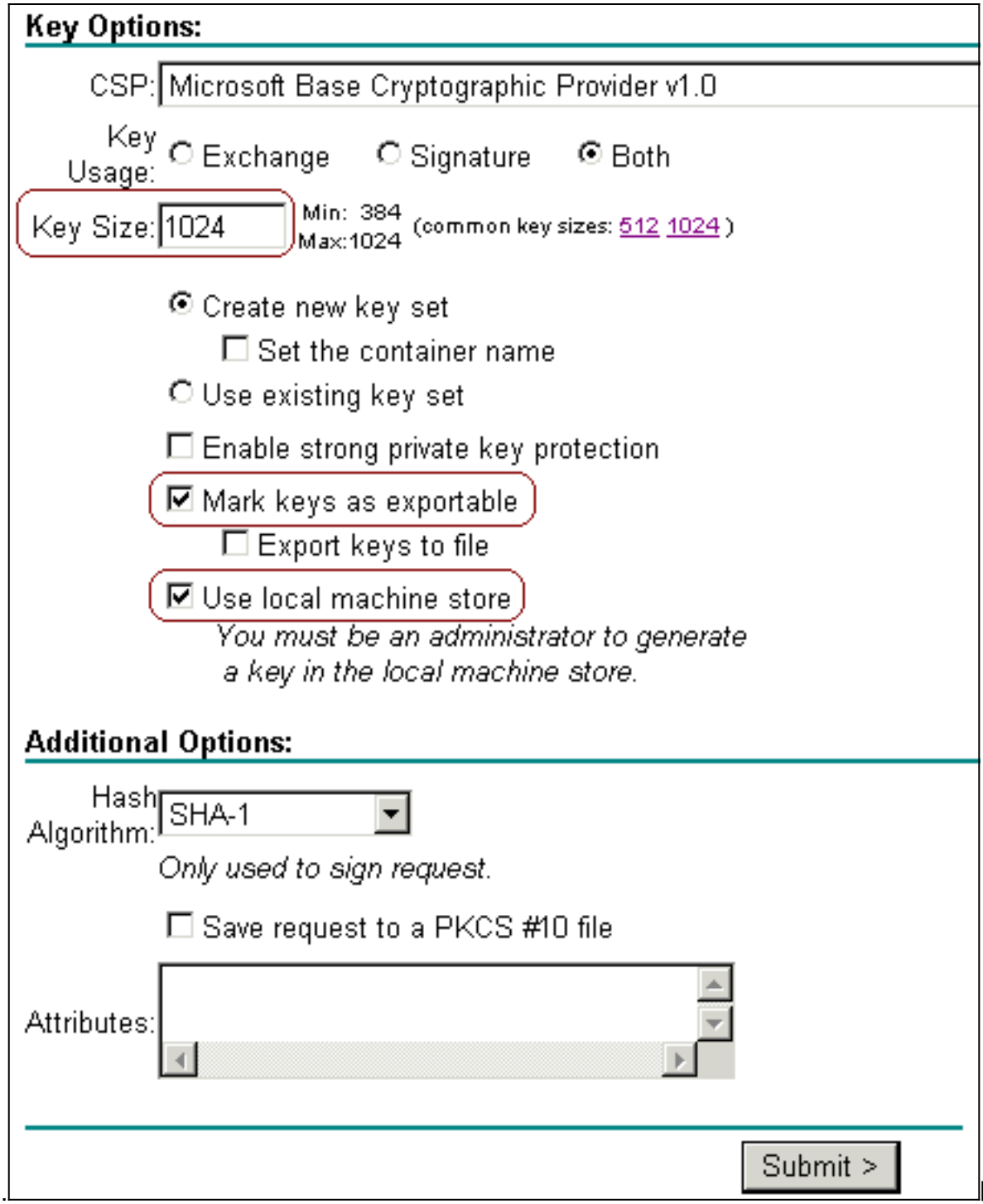


Weiter.

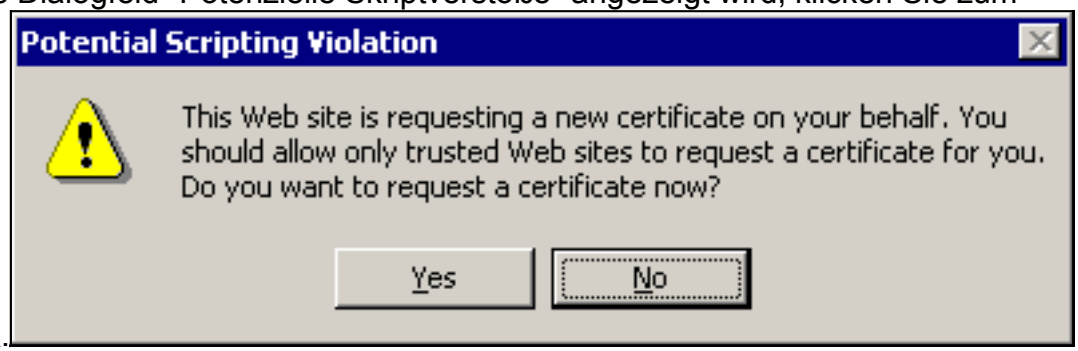
6. Konfigurieren Sie die Zertifikatoptionen:Wählen Sie **Webserver** als Zertifikatsvorlage aus, und geben Sie den Namen des ACS-Servers



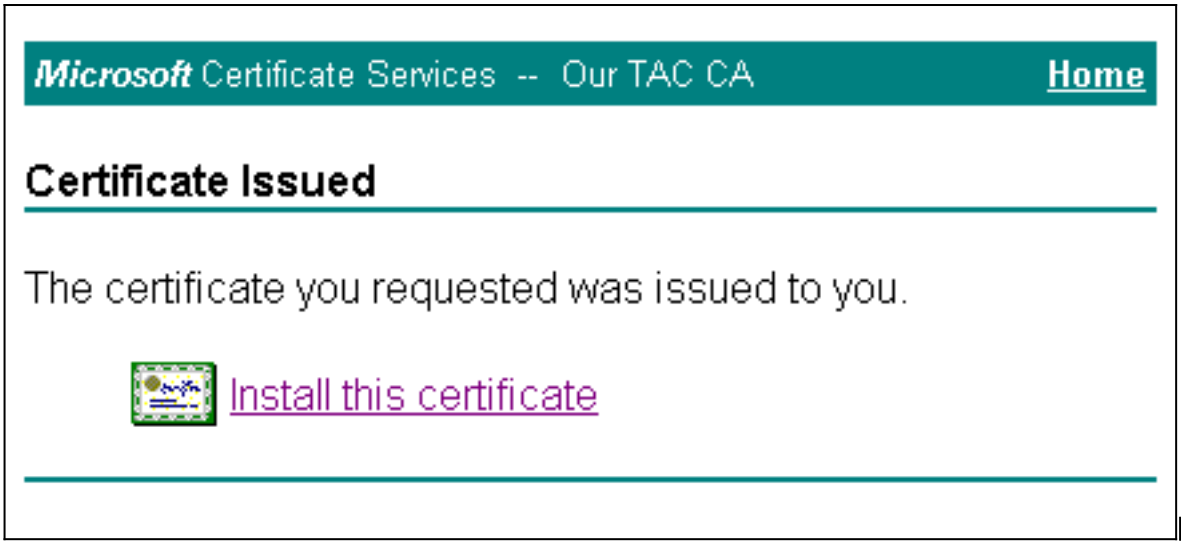
ein.Geben Sie **1024** im Feld Schlüsselgröße ein, und aktivieren Sie die Kontrollkästchen **Schlüssel als exportierbar markieren** und **Lokalen Maschinenspeicher verwenden**.Konfigurieren Sie nach Bedarf weitere Optionen, und klicken Sie dann auf



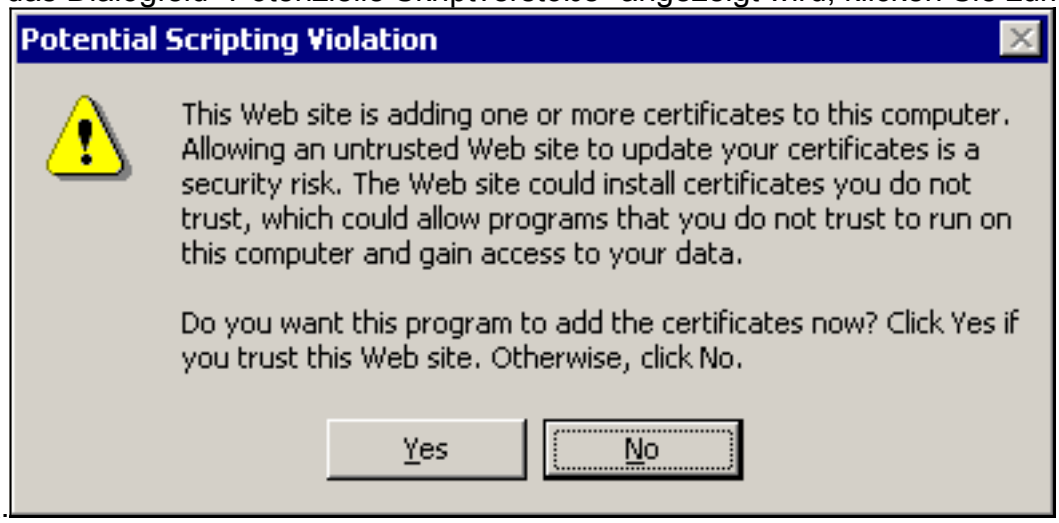
Senden.**Hinweis:** Wenn das Dialogfeld "Potenzielle Skriptverstöße" angezeigt wird, klicken Sie zum Fortfahren auf **Ja**.



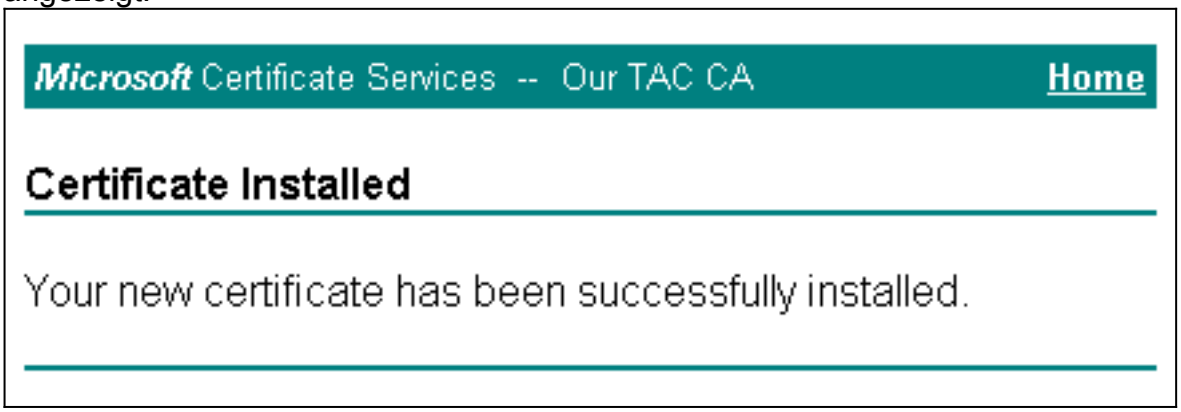
7. Klicken Sie auf **Zertifikat installieren**.



Hinweis: Wenn das Dialogfeld "Potenzielle Skriptverstöße" angezeigt wird, klicken Sie zum Fortfahren auf **Ja**.



8. Wenn die Installation erfolgreich war, wird die Meldung Certificate Installed (Zertifikat installiert) angezeigt.

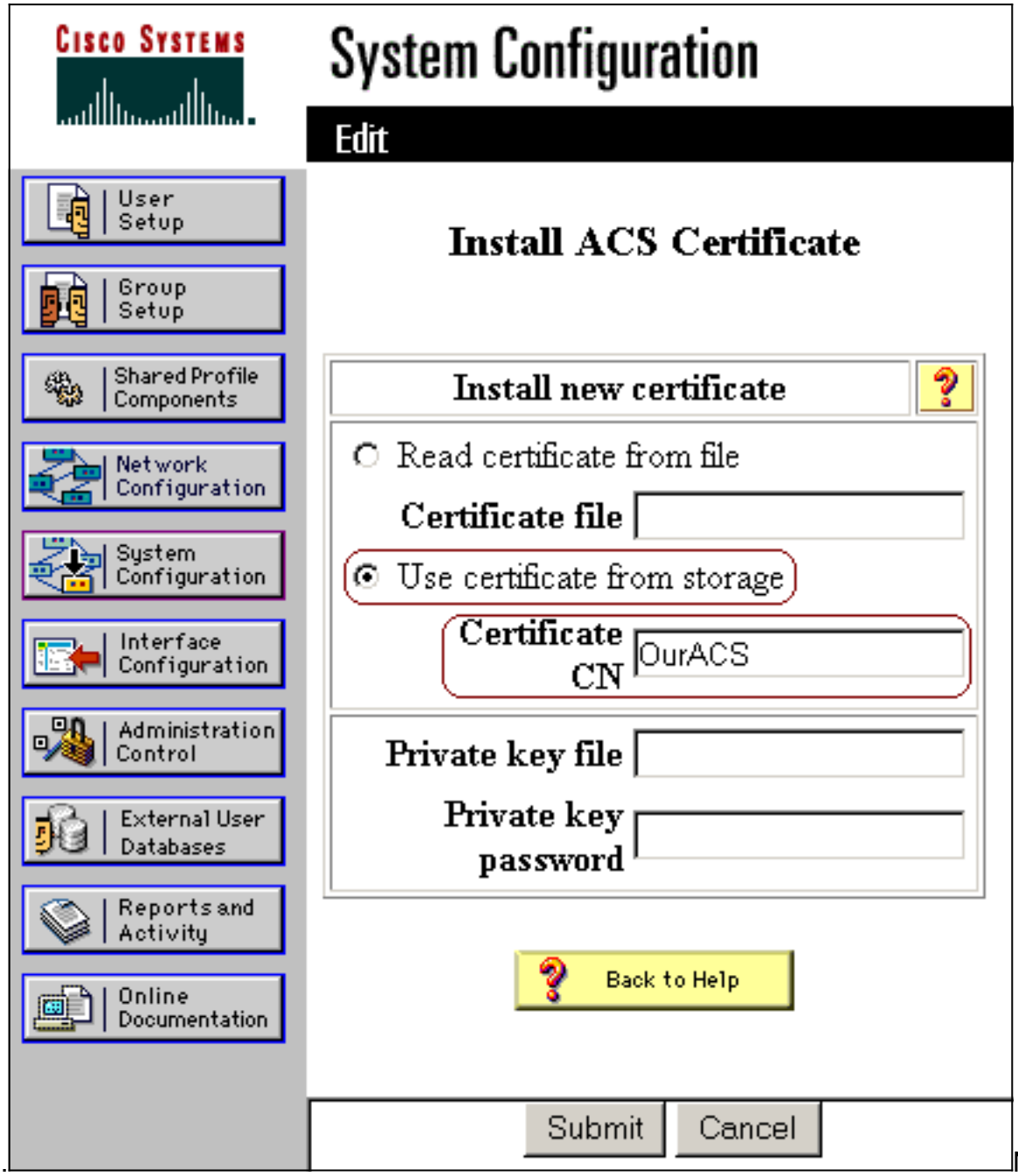


Konfigurieren des ACS zur Verwendung eines Zertifikats aus dem Speicher

Führen Sie diese Schritte aus, um ACS für die Verwendung des Zertifikats im Speicher zu konfigurieren.

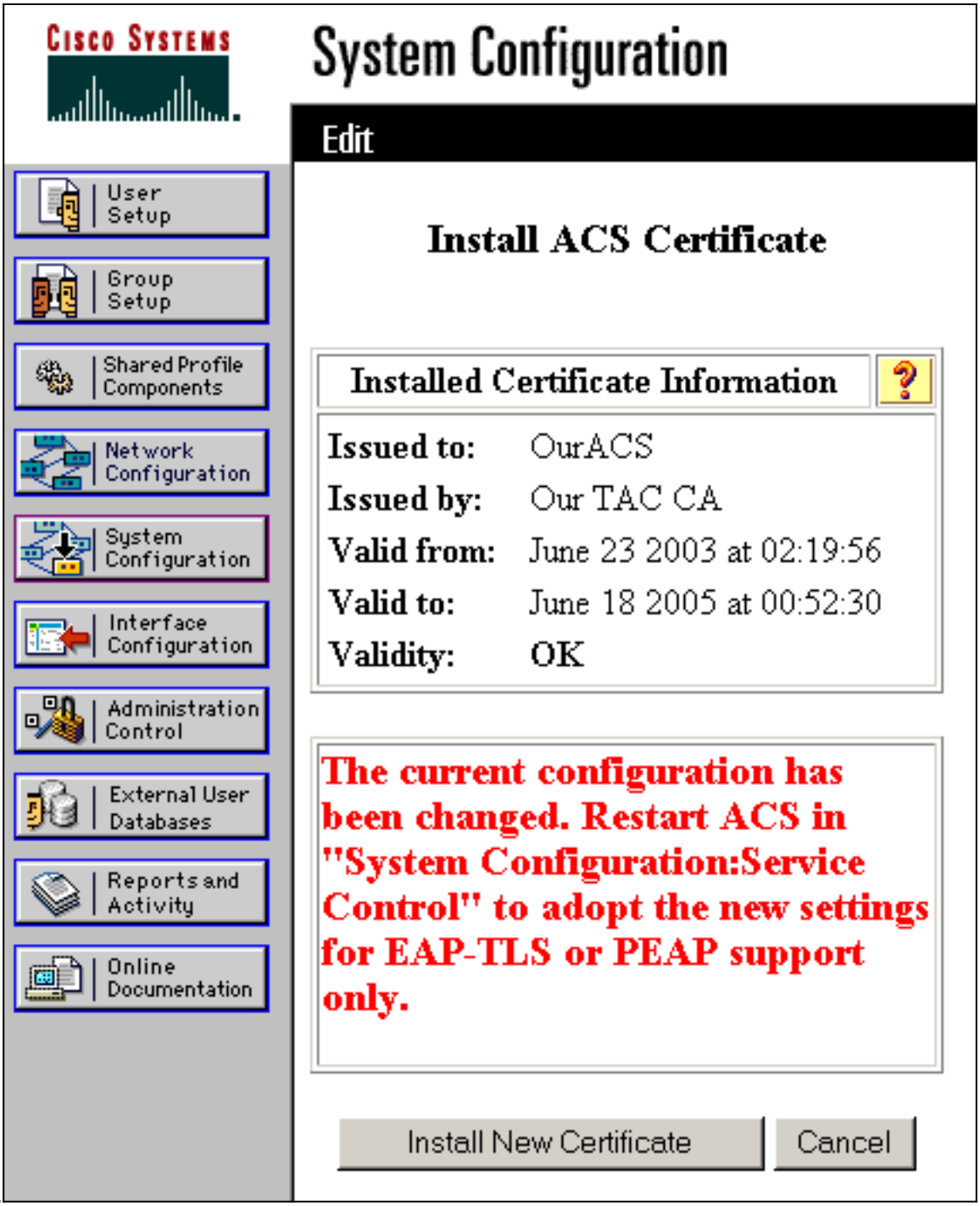
1. Öffnen Sie einen Webbrowser, und geben Sie **http://*ACS-ip-address*:2002/** ein, um auf den ACS-Server zuzugreifen.
2. Klicken Sie auf **Systemkonfiguration** und dann auf **ACS Certificate Setup**.
3. Klicken Sie auf **ACS-Zertifikat installieren**.

4. Klicken Sie auf das Optionsfeld **Zertifikat vom Speicher verwenden**.
5. Geben Sie im Feld Certificate CN (CN-Zertifikat) den Namen des Zertifikats ein, das Sie in Schritt 5a des Abschnitts Obtain a Certificate From the ACS Server (Zertifikat vom ACS-Server beziehen) dieses Dokuments zugewiesen haben.
6. Klicken Sie auf



Senden.Nach Abschluss der Konfiguration wird eine Bestätigungsmeldung angezeigt, die anzeigt, dass die Konfiguration des ACS-Servers geändert wurde.**Hinweis:** Sie müssen den ACS derzeit nicht neu

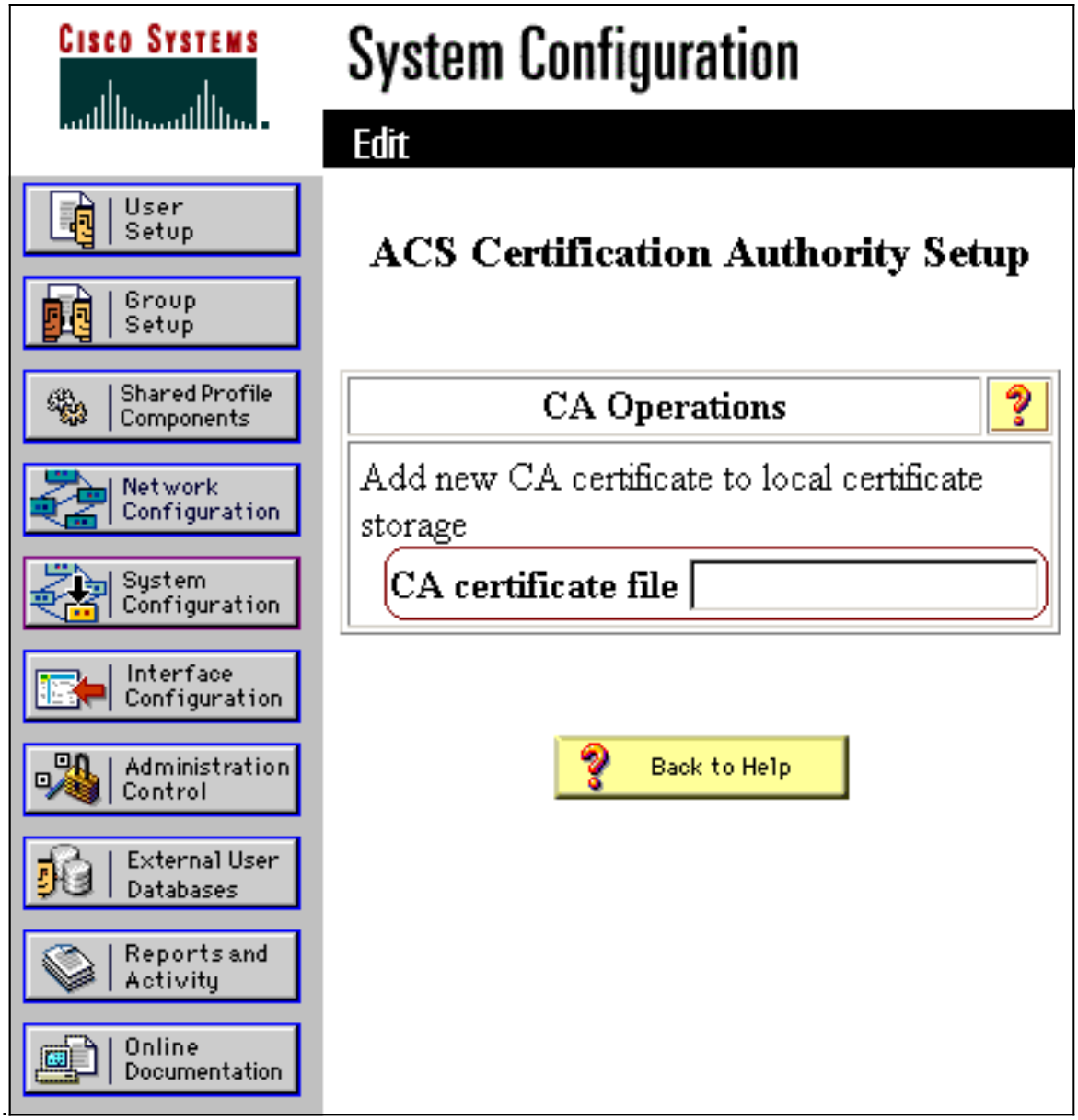
starten.



Angeben zusätzlicher Zertifizierungsstellen, denen der ACS vertrauen sollte

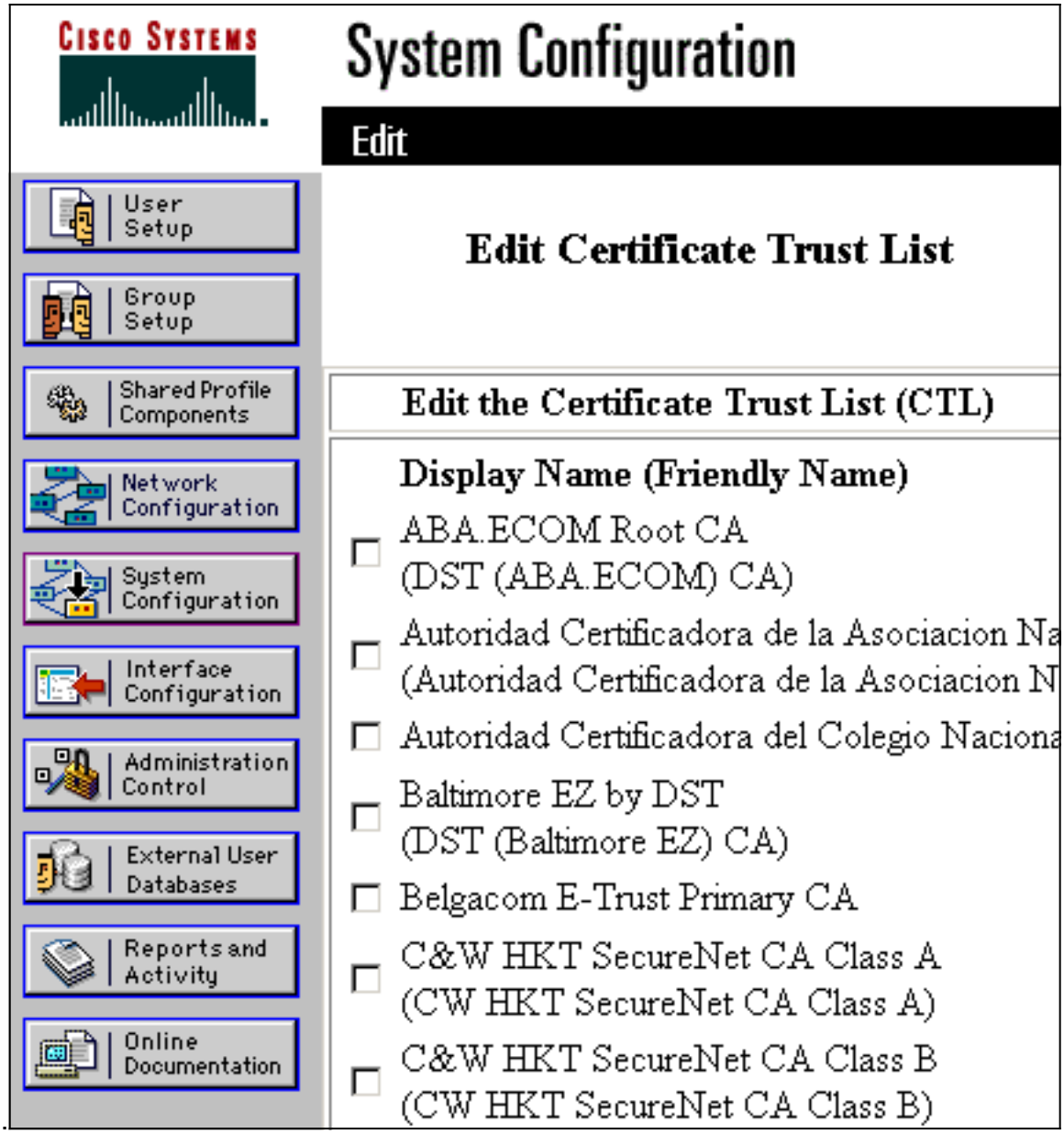
Der ACS vertraut automatisch der Zertifizierungsstelle, die ein eigenes Zertifikat ausgestellt hat. Wenn die Client-Zertifikate von zusätzlichen Zertifizierungsstellen ausgestellt werden, müssen Sie die folgenden Schritte ausführen:

1. Klicken Sie auf **Systemkonfiguration** und dann auf **ACS Certificate Setup**.
2. Klicken Sie auf **ACS Certificate Authority Setup**, um der Liste der vertrauenswürdigen Zertifikate CAs hinzuzufügen.
3. Geben Sie im Feld für Zertifizierungsstellenzertifikatdatei den Speicherort des Zertifikats ein, und klicken Sie dann auf



Senden.

4. Klicken Sie auf **Liste der Zertifikatsvertrauenslisten bearbeiten**.
5. Überprüfen Sie alle CAs, denen der ACS vertrauen soll, und deaktivieren Sie alle CAs, denen der ACS nicht vertrauen darf.
6. Klicken Sie auf



Senden.

Starten Sie den Dienst neu, und konfigurieren Sie die EAP-TLS-Einstellungen auf dem ACS.

Gehen Sie wie folgt vor, um den Service neu zu starten und die EAP-TLS-Einstellungen zu konfigurieren:

1. Klicken Sie auf **Systemkonfiguration** und dann auf **Dienststeuerung**.
2. Klicken Sie auf **Neu starten**, um den Dienst neu zu starten.
3. Um EAP-TLS-Einstellungen zu konfigurieren, klicken Sie auf **Systemkonfiguration** und dann auf **Globales Authentifizierungs-Setup**.
4. Aktivieren Sie **EAP-TLS zulassen**, und überprüfen Sie dann einen oder mehrere Zertifikatvergleiche.
5. Klicken Sie auf