EAP-TLS マシン認証を使用する Windows v3.2 の Secure ACS

目次

はじめに

このドキュメントでは、Cisco Secure Access Control System（ACS）for Windows バージョン 3.2 を使用して、Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）を設定する方法を説明します。

注: Novell 認証局（CA）によるマシン認証はサポートされません。 ACS は、EAP-TLS を使用して、Microsoft Windows Active Directory に対するマシン認証をサポートすることができます。 エンドユーザ クライアントは、ユーザ認証のプロトコルを、マシン認証に使用するプロトコルと同じものに制限する場合があります。 その場合、マシン認証に EAP-TLS を使用するとしたら、ユーザ認証にも EAP-TLS を使用する必要があります。 マシン認証に関する詳細については、『*Cisco Secure Access Control Server 4.1 ユーザ ガイド*』の「マシン認証」のセクションを参照し

てください。

注: EAP-TLS でマシンを認証するように ACS をセットアップする場合、その ACS がマシン認証用にセットアップされているとしたら、クライアントをマシン認証専用に設定する必要があります。 詳細については、「Windows Vista、Windows Server 2008 、および Windows XP Service Pack 3 で、802.1 X ベースのネットワーク用のコンピューターのみの認証を有効にする方法」を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Secure ACS for Windows バージョン 3.2
- Microsoft Certificate Services (エンタプライズのルート証明機関 [CA] としてインストールされている) **注:** 詳細については、認証局のセットアップに関する手順ガイド を参照してください。
- Service Pack 3 およびホットフィックス 323172 を適用済みの Windows 2000 Server を使用した DNS サービス**注:** CA サーバの問題が発生した場合は、ホットフィックス 323172 をインストールします。 Windows 2000 SP3 クライアントでは、ホットフィックス 313664 を適用しないと IEEE 802.1x 認証を有効にできません。
- Cisco Aironet 1200 シリーズ Wireless Access Point 12.01T
- Service Pack 1 を適用済みの Windows XP Professional を実行する IBM ThinkPad T30

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景理論

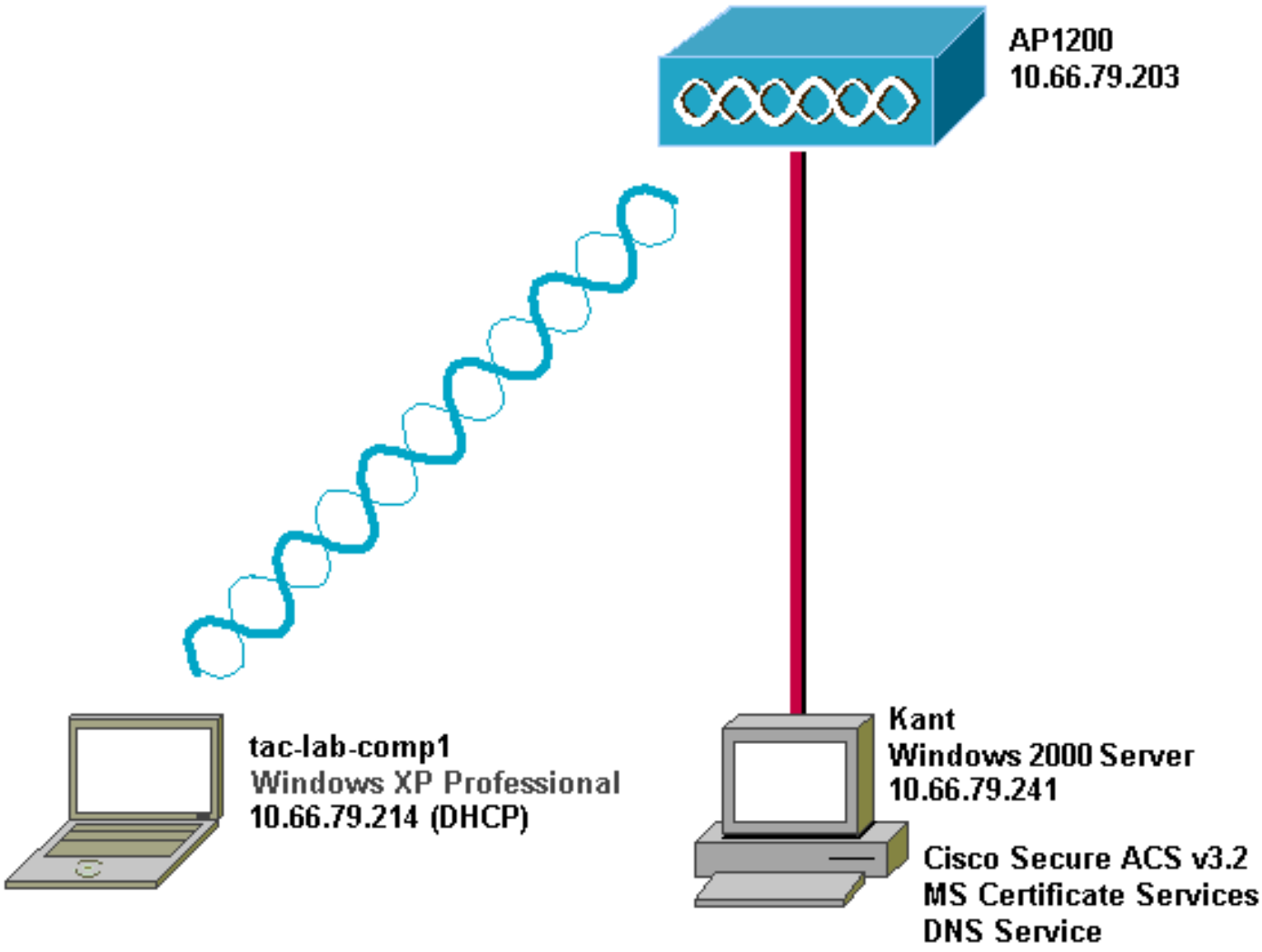
EAP-TLS と Protected Extensible Authentication Protocol (PEAP) は両方とも、TLS/Secure Socket Layer (SSL; セキュア ソケット レイヤ) トンネルを構築し、使用します。 EAP-TLS では、ACS (Authentication, Authorization, and Accounting (AAA; 認証、認可、およびアカウンティング)) サーバとクライアントの両方が証明書を用意し、相互に ID を証明する相互認証を使用します。 ただし、PEAP が使用するのはサーバ側の認証だけです。 サーバだけが証明書を所有し、その ID をクライアントに証明します。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

ネットワーク図

このドキュメントでは次の図に示すネットワーク



Cisco Secure ACS for Windows v3.2 の設定

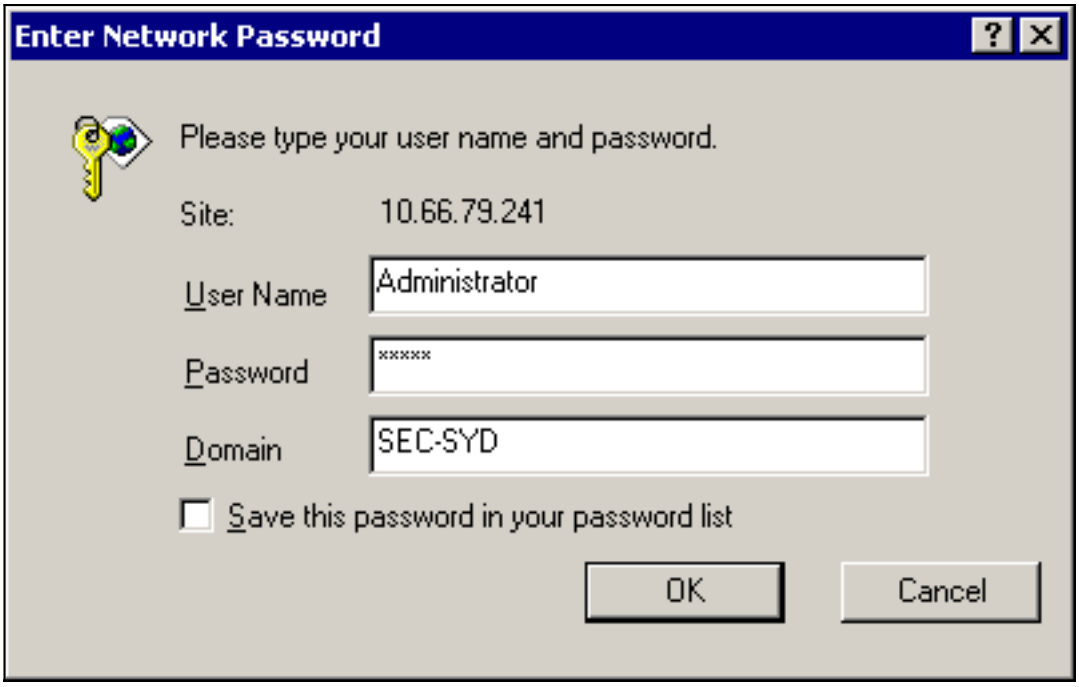
ACS 3.2 を設定するには、次のステップに従います。

1. ACS サーバ用の証明書を取得する。
2. ストレージから証明書を使用するよう ACS を設定する。
3. ACS が信頼する必要のある追加の認証局を指定する。
4. サービスを再起動し、ACS での EAP-TLS 設定を構成する。
5. アクセス ポイントを AAA クライアントとして指定および設定する。
6. 外部ユーザ データベースを設定する。
7. サービスを再起動する。

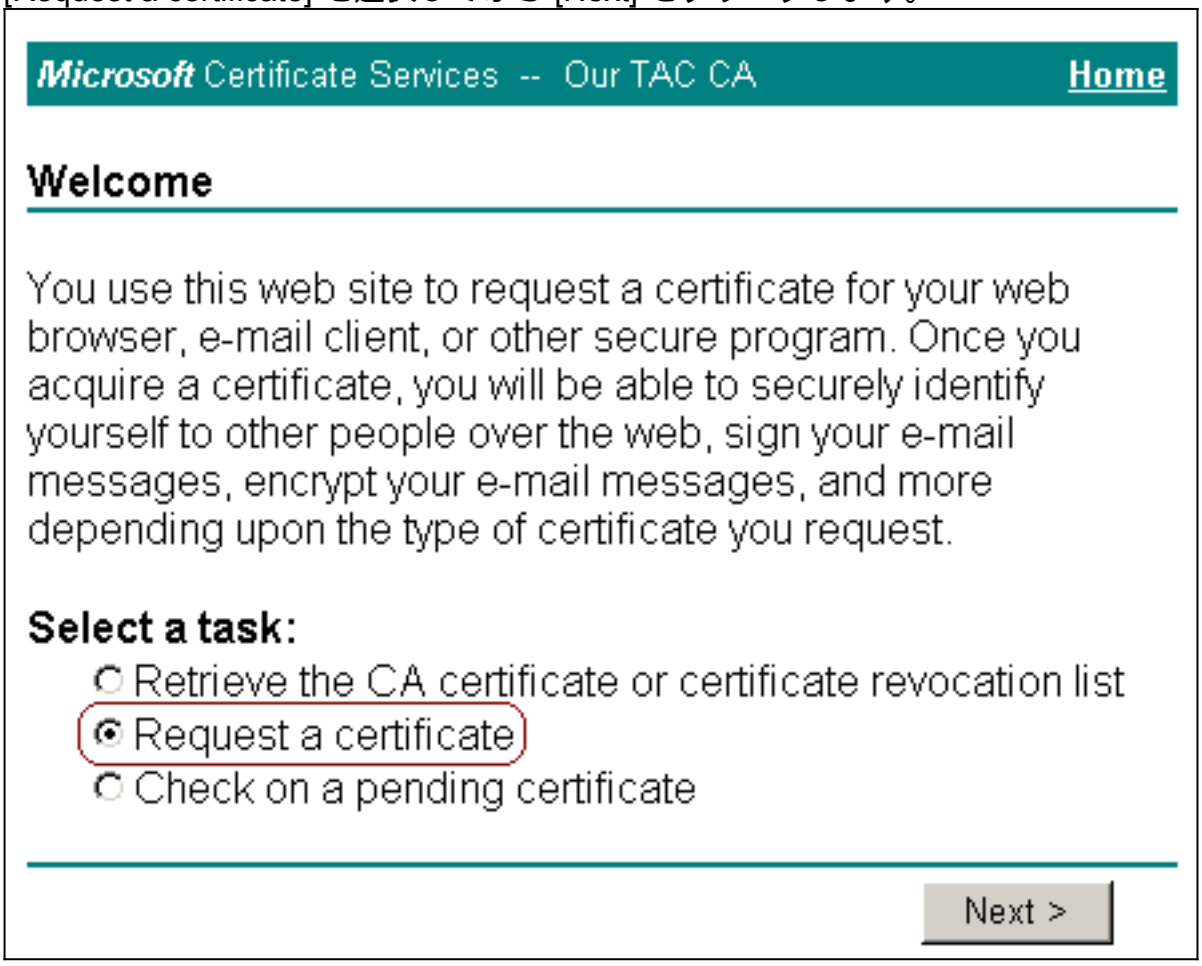
ACS サーバ用の証明書を取得する

証明書を取得するには、次のステップに従います。

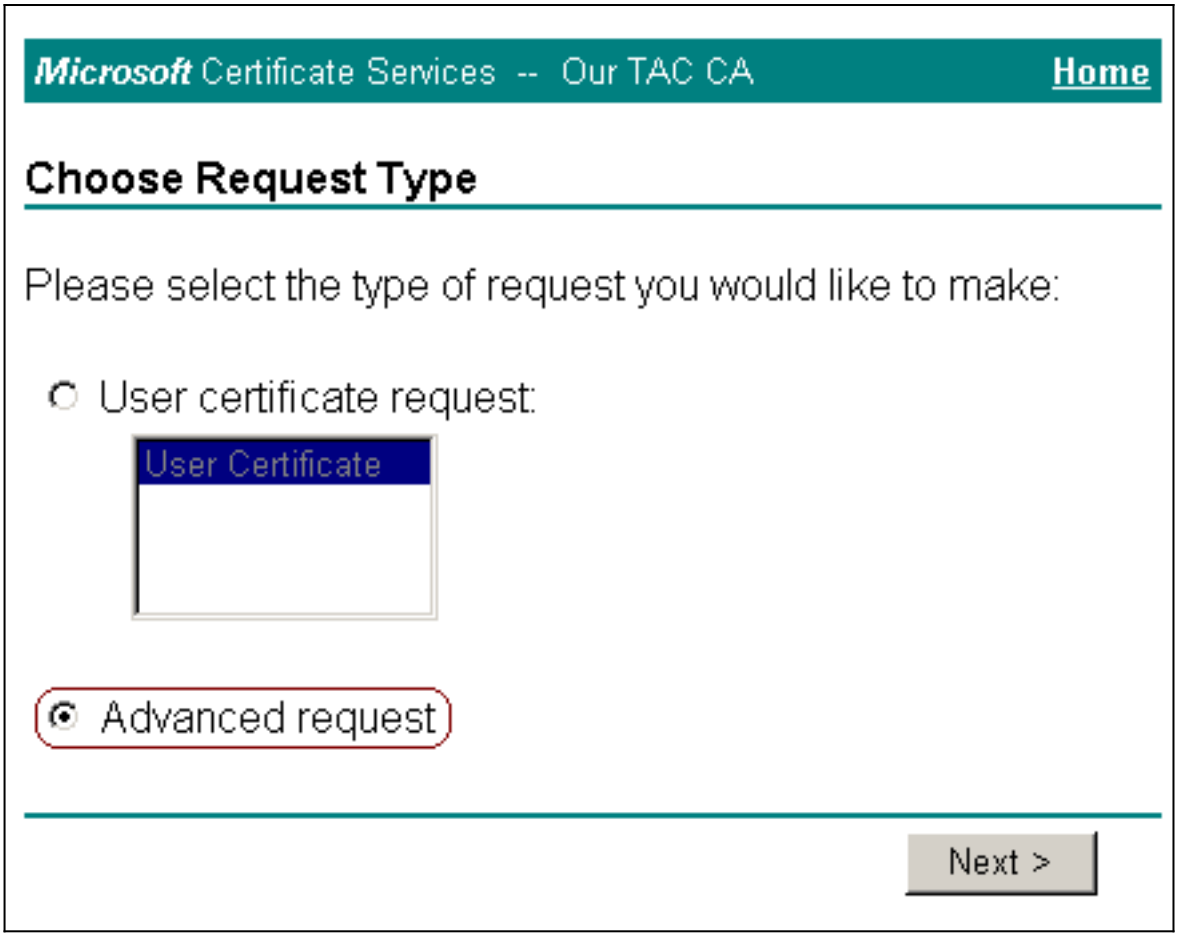
1. ACS サーバで Web ブラウザを開き、CA サーバにアクセスするためにアドレス バーに **http://CA-ip-address/certsrv** と入力します。
2. Administrator としてドメインにログインします。



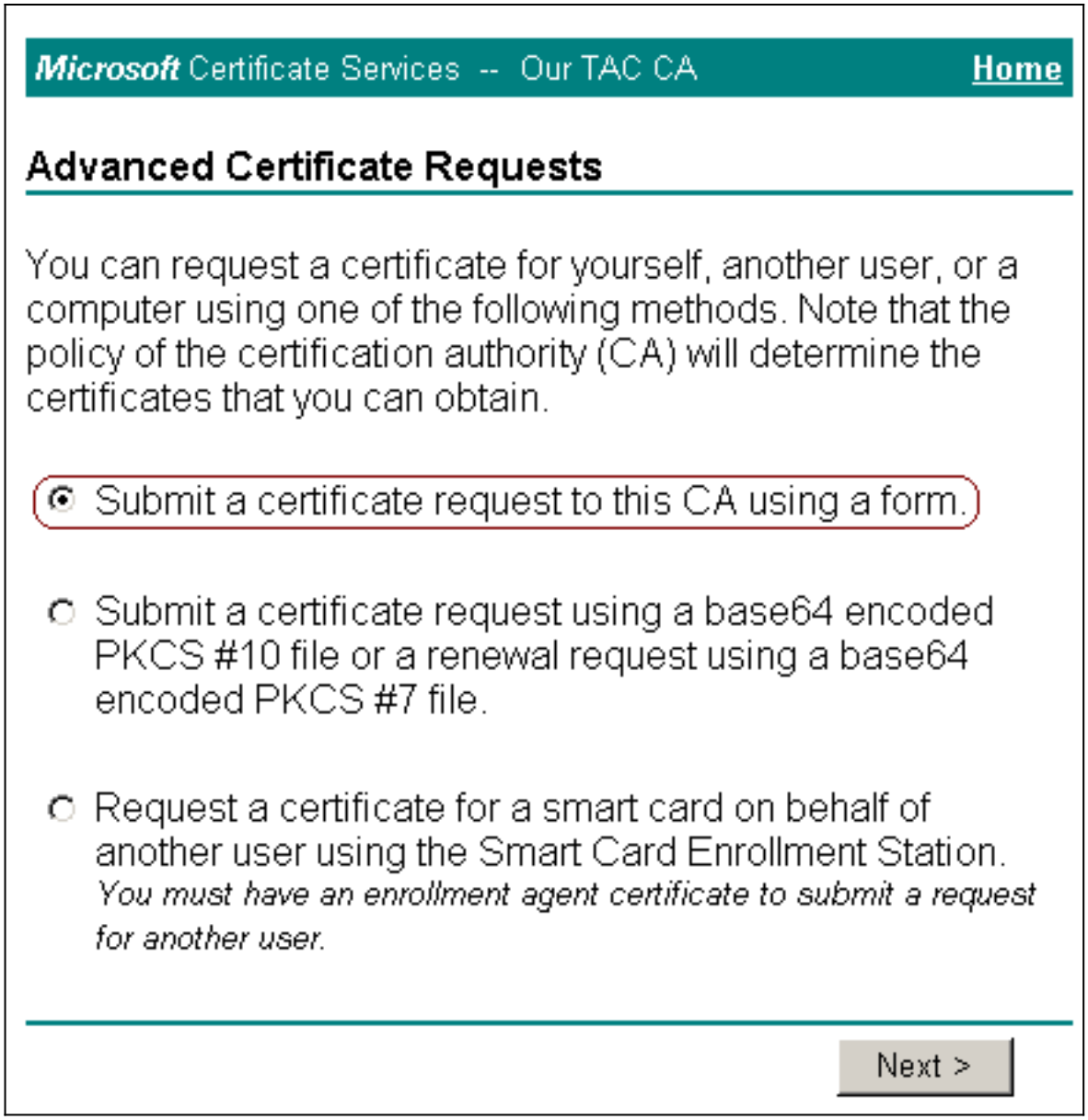
3. [Request a certificate] を選択してから [Next] をクリックします。



4. [Advanced request] を選択してから [Next] をクリックします。

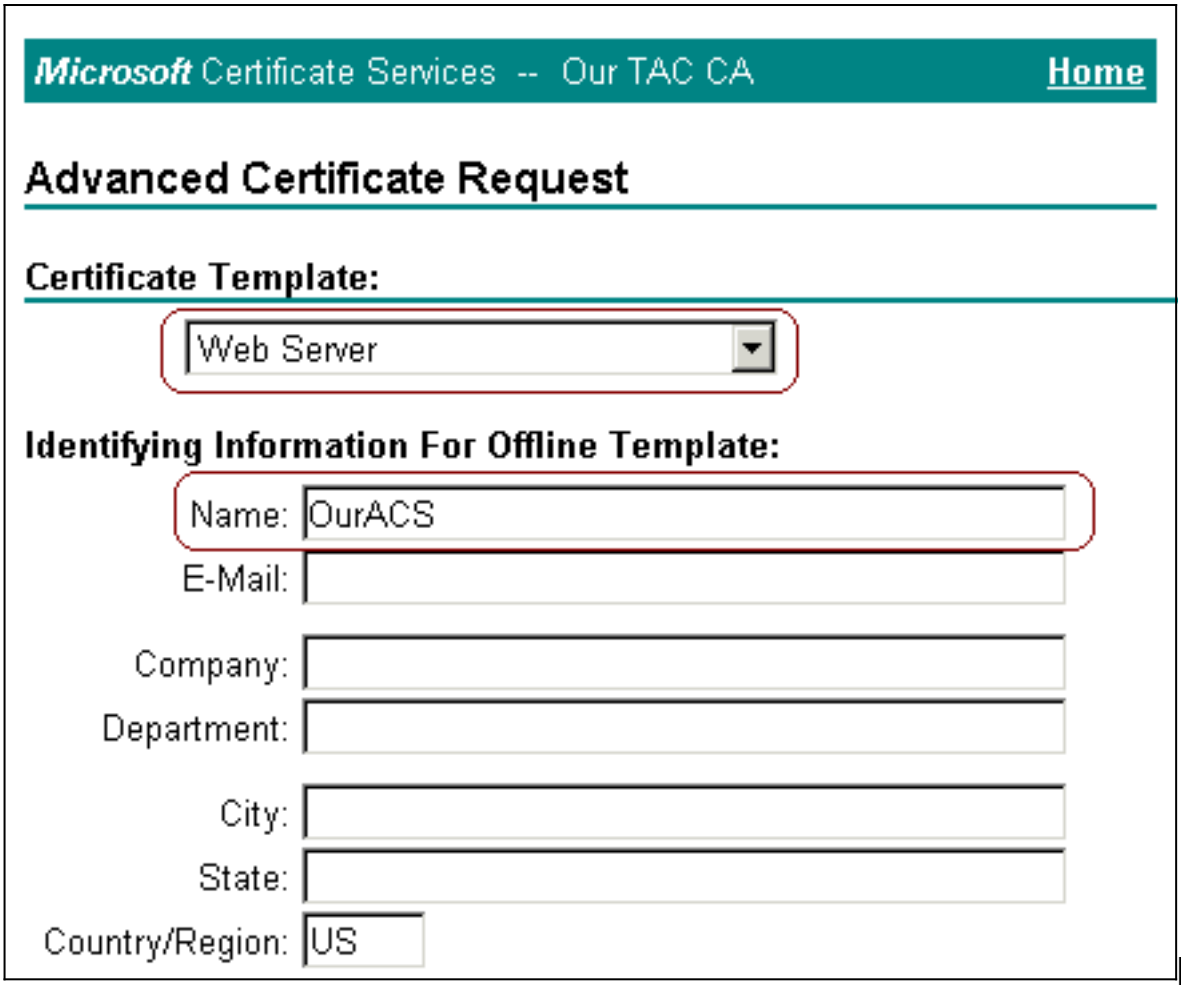


5. [Submit a certificate request to this CA using a form] を選択してから [Next] をクリックしま

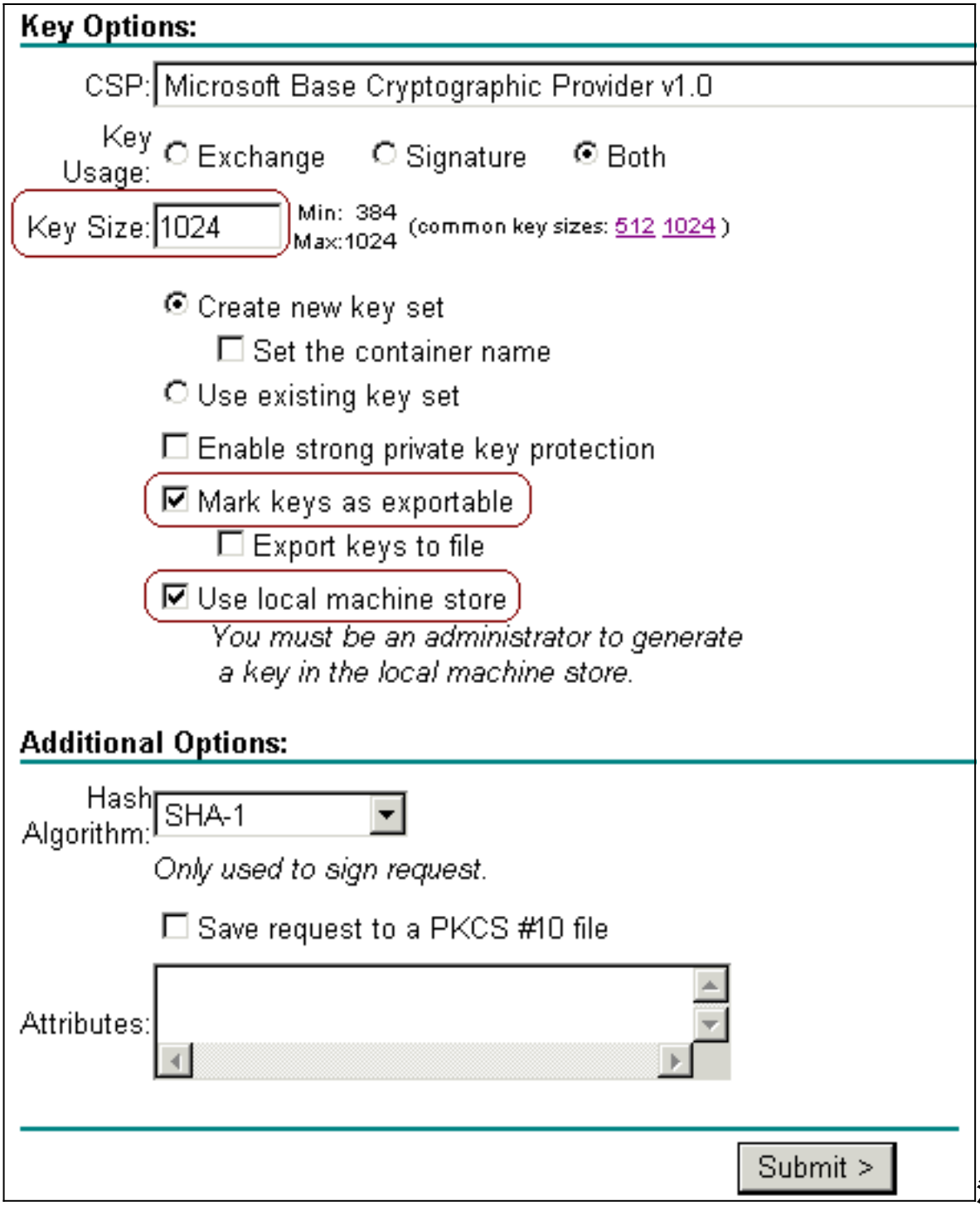


す。

6. 証明書のオプションを設定します。証明書のテンプレートとして [Web Server] を選択し、ACS サーバの名前を入力します。

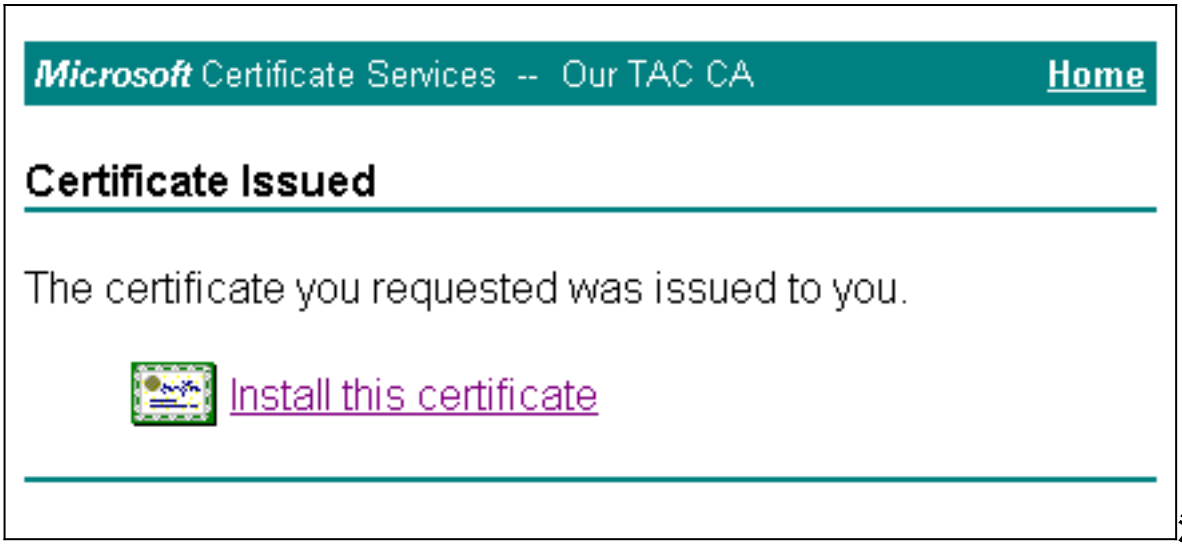


[Key Size] フィールドに 1024 と入力し、[Mark keys as exportable] および [Use local machine store] チェックボックスをオンにします。必要に応じてその他のオプションを設定し、[Submit] をクリックします。

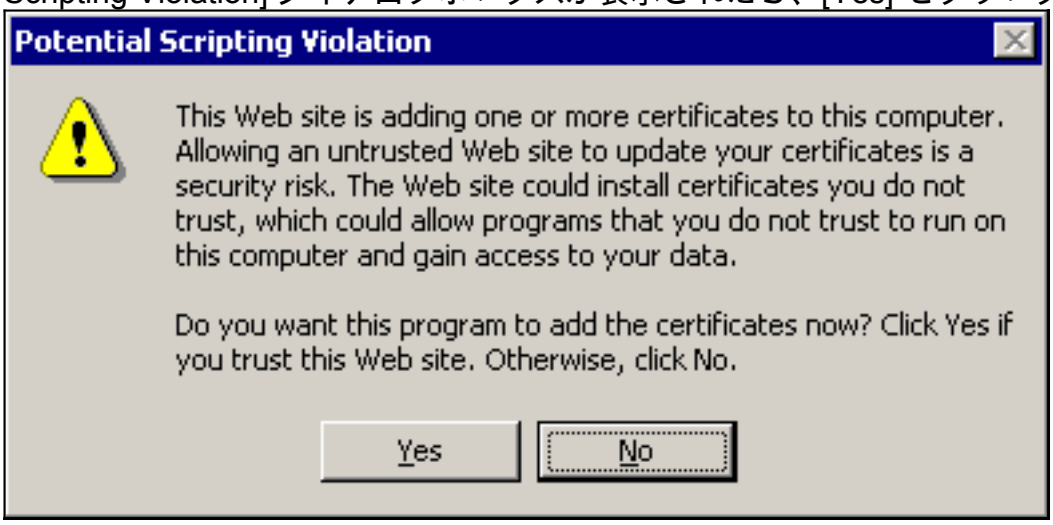


注: [Potential Scripting Violation] ダイアログボックスが表示されたら、[Yes] をクリックして続行します。

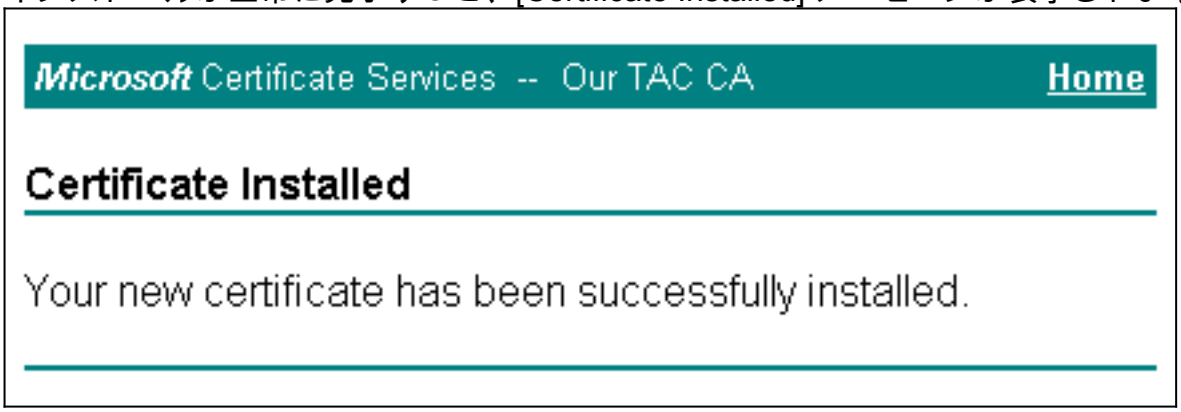
7. [Install this certificate] をクリックします。



注: [Potential Scripting Violation] ダイアログボックスが表示されたら、[Yes] をクリックして続行します。



8. インストールが正常に完了すると、[Certificate Installed] メッセージが表示されます。

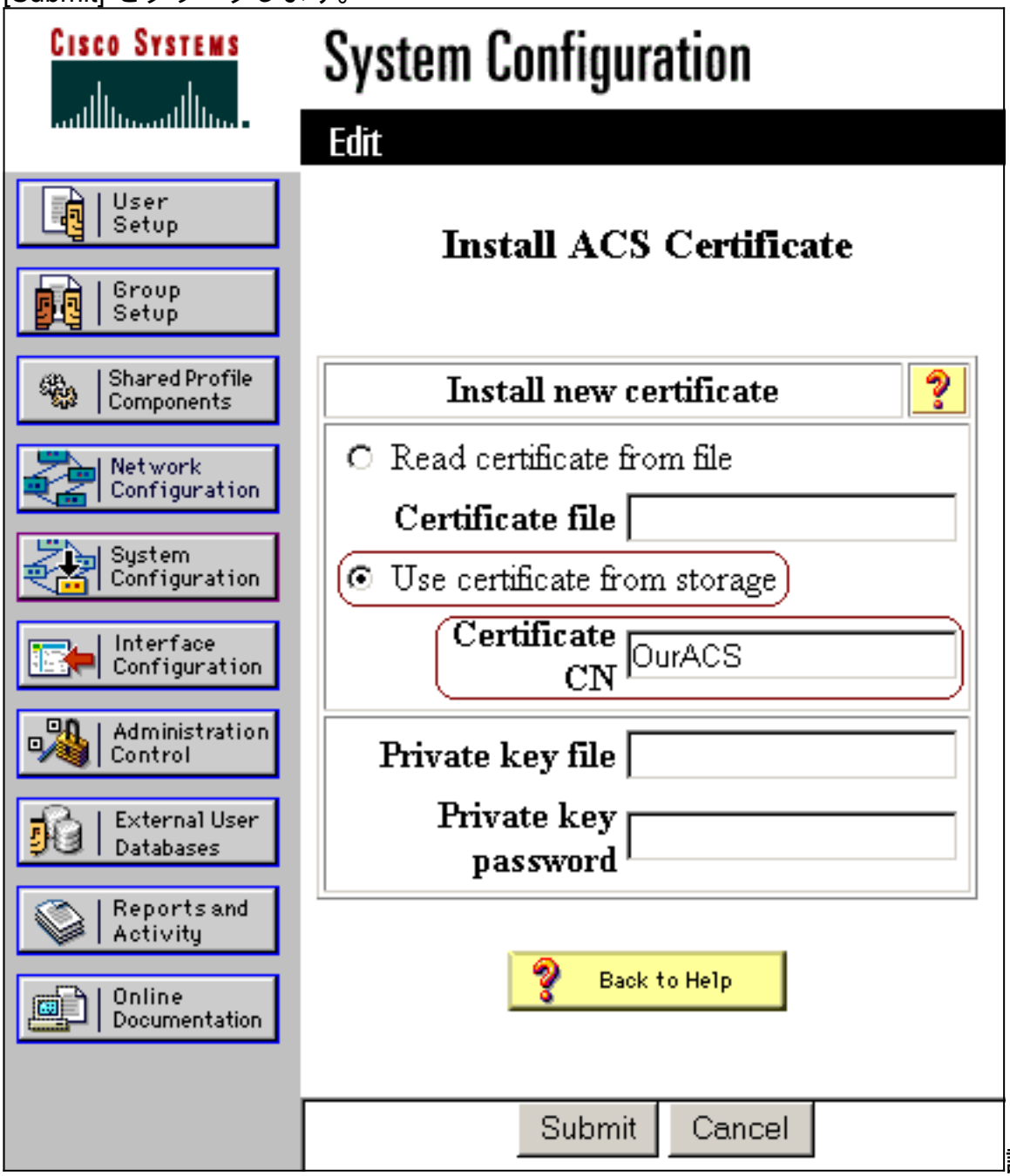


ストレージから証明書を使用するよう ACS を設定する

ストレージにある証明書を使用するよう ACS を設定するには、次のステップに従います。

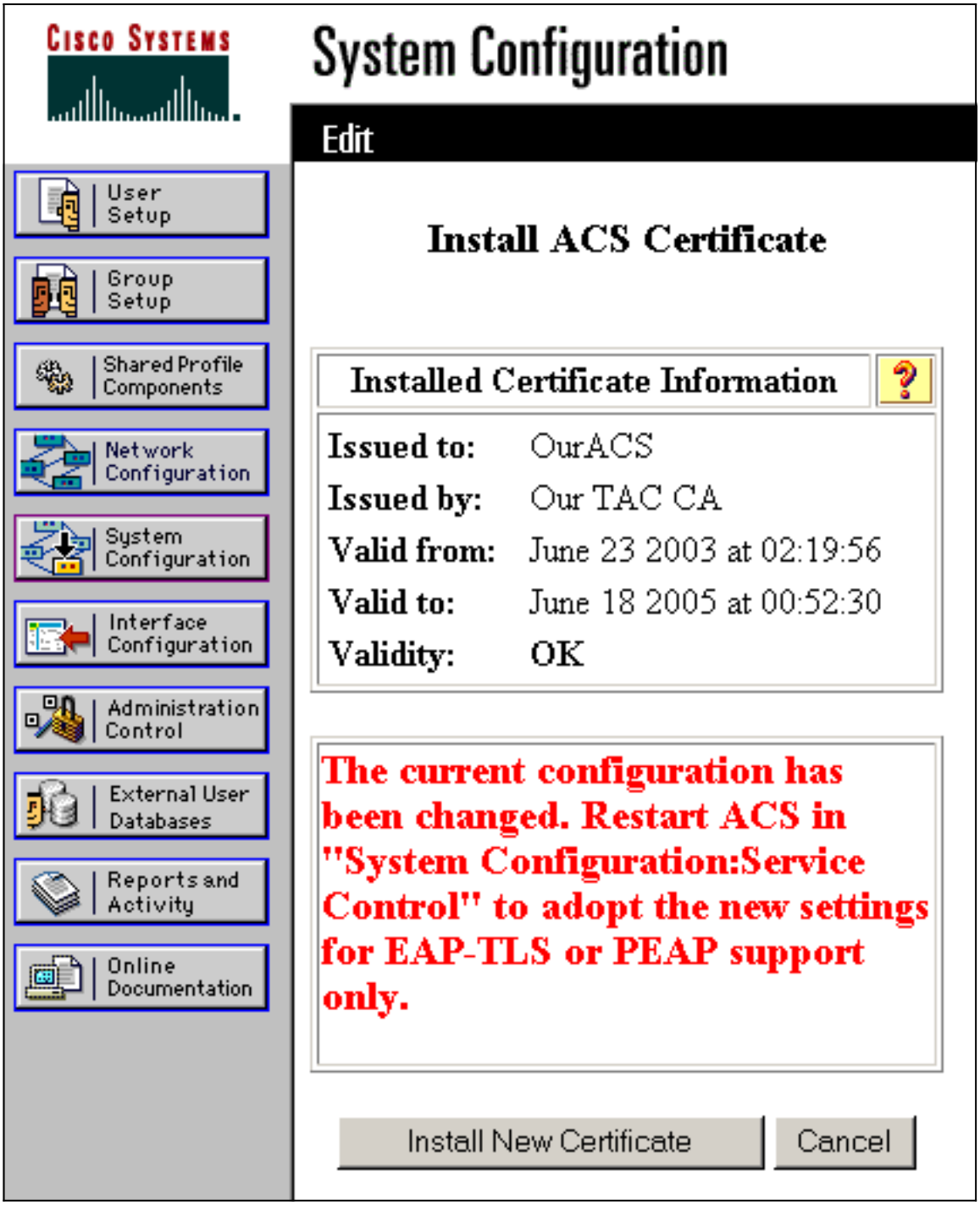
1. Web ブラウザを開き、ACS サーバにアクセスするためにアドレス バーに **http://*ACS-ip-address:2002/*** と入力します。
2. [System Configuration] をクリックし、[ACS Certificate Setup] をクリックします。
3. [Install ACS Certificate] をクリックします。
4. [Use certificate from storage] オプション ボタンをクリックします。
5. [Certificate CN] フィールドに、このドキュメントの「ACS サーバ用の証明書を取得する」セクションのステップ 5a で割り当てた証明書の名前を入力します。

6. [Submit] をクリックします。



設定が完了すると、ACS サーバの設定が変更されたことを通知する確認メッセージが表示されます。

注: この時点では ACS を再起動する必要はありません。



ACS が信頼する必要のある追加の認証局を指定する

ACS は、自身の証明書を発行した CA を自動的に信頼します。 クライアント証明書が別の CA により発行された場合は、次のステップを完了する必要があります。

1. [System Configuration] をクリックし、[ACS Certificate Setup] をクリックします。
2. ACS Certificate Authority Setup をクリックして、信頼された証明書のリストに CA を追加します。
3. CA 証明書ファイル用のフィールドに証明書の場所を入力し、[Submit] をクリックします。

4. [Edit Certificate Trust List] をクリックします。
5. ACS が信頼するすべての CA にチェック マークを付け、ACS が信頼しないすべての CA のチェック マークを外します。
6. [Submit] をクリックします。

サービスを再起動し、ACS での EAP-TLS 設定を構成する

サービスを再起動して EAP-TLS 設定を構成するには、次のステップに従います。

1. [System Configuration] をクリックし、[Service Control] をクリックします。
2. [Restart] をクリックしてサービスを再起動します。
3. EAP-TLS 設定を構成するために、[System Configuration] をクリックし、[Global Authentication Setup] をクリックします。
4. [Allow EAP-TLS] チェックボックスをオンにしてから、1 つ以上の証明書比較にチェック マークを付けます。
5. [Submit] をクリックします。