PEAP-MS-CHAPv2 マシン認証が設定された Cisco Secure ACS for Windows v3.2

目次

概要

この文書では、Cisco Secure ACS for Windows バージョン 3.2 を使用して、Protected Extensible Authentication Protocol（PEAP）を設定する方法を説明します。

ワイヤレス LAN コントローラを使用してセキュア ワイヤレスアクセスを、Microsoft Windows 2003 ソフトウェア設定する方法に関する詳細についてはおよび Cisco Secure Access Control Server（ACS）4.0 は ACS 4.0 および Windows 2003 が付いている Unified Wireless Network の下で、PEAP を示します。

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 をインストールした Windows 2000 Server を使った 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、クリアな（デフォルト）設定で作業を開始しています。 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

PEAP と EAP-TLS は両方とも TLS/Secure Socket Layer（SSL）トンネルを構築して、使用します。 PEAP はサーバ側の認証だけ使用します; 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。 しかし 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。

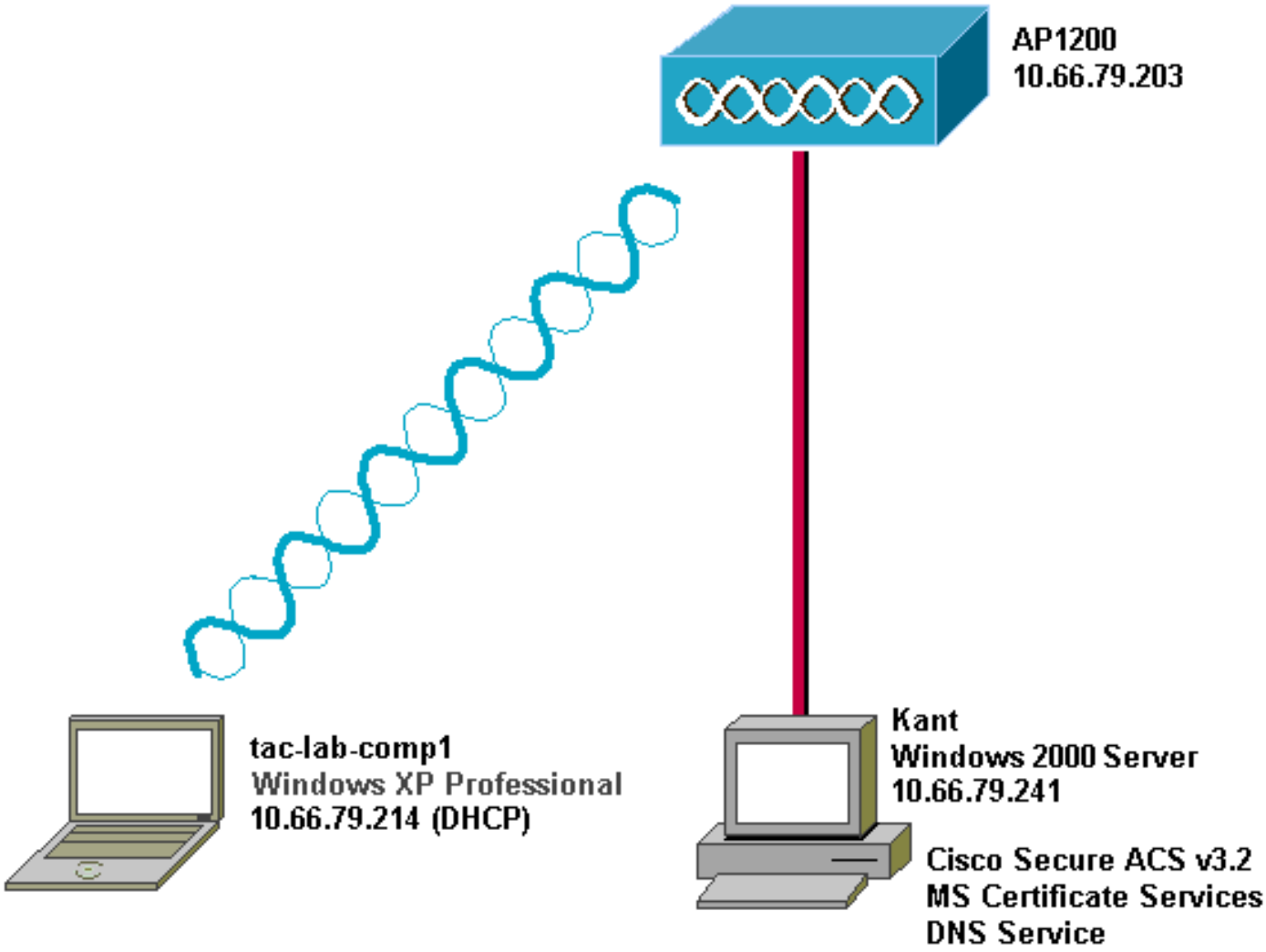
クライアントが証明書を必要としないため、PEAP は便利です。 EAP-TLS は、証明書がユーザからのインタラクションを必要とないため、認証を行うヘッドレス デバイスでは有用です。

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



設定 Cisco Secure ACS for Windows v3.2

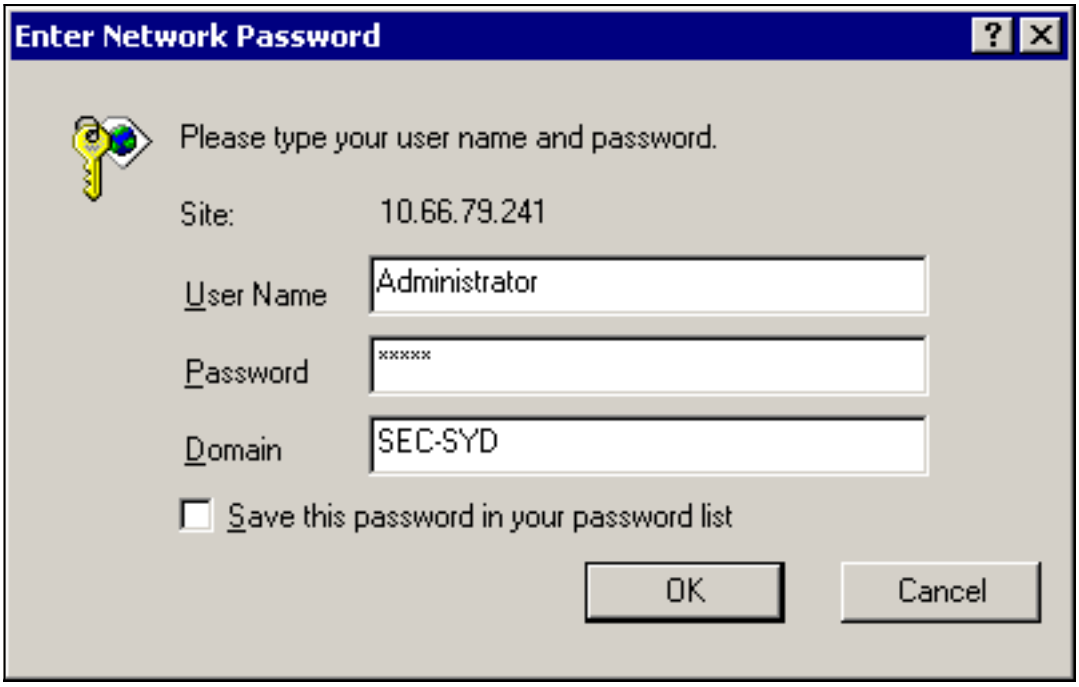
ACS 3.2 を設定するために次の手順に従って下さい。

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。

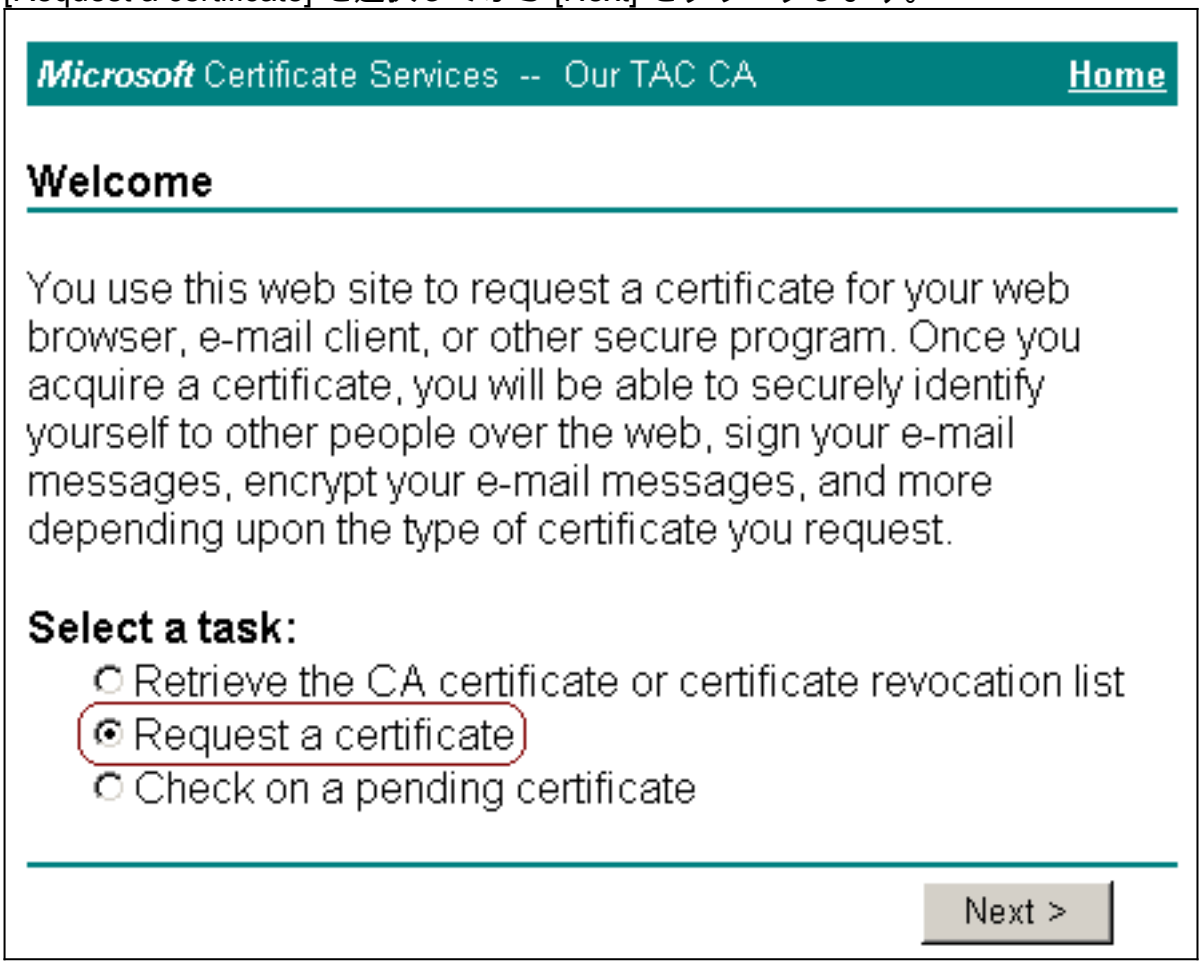
ACS サーバ用の証明書を取得する

証明書を取得するには、次のステップに従います。

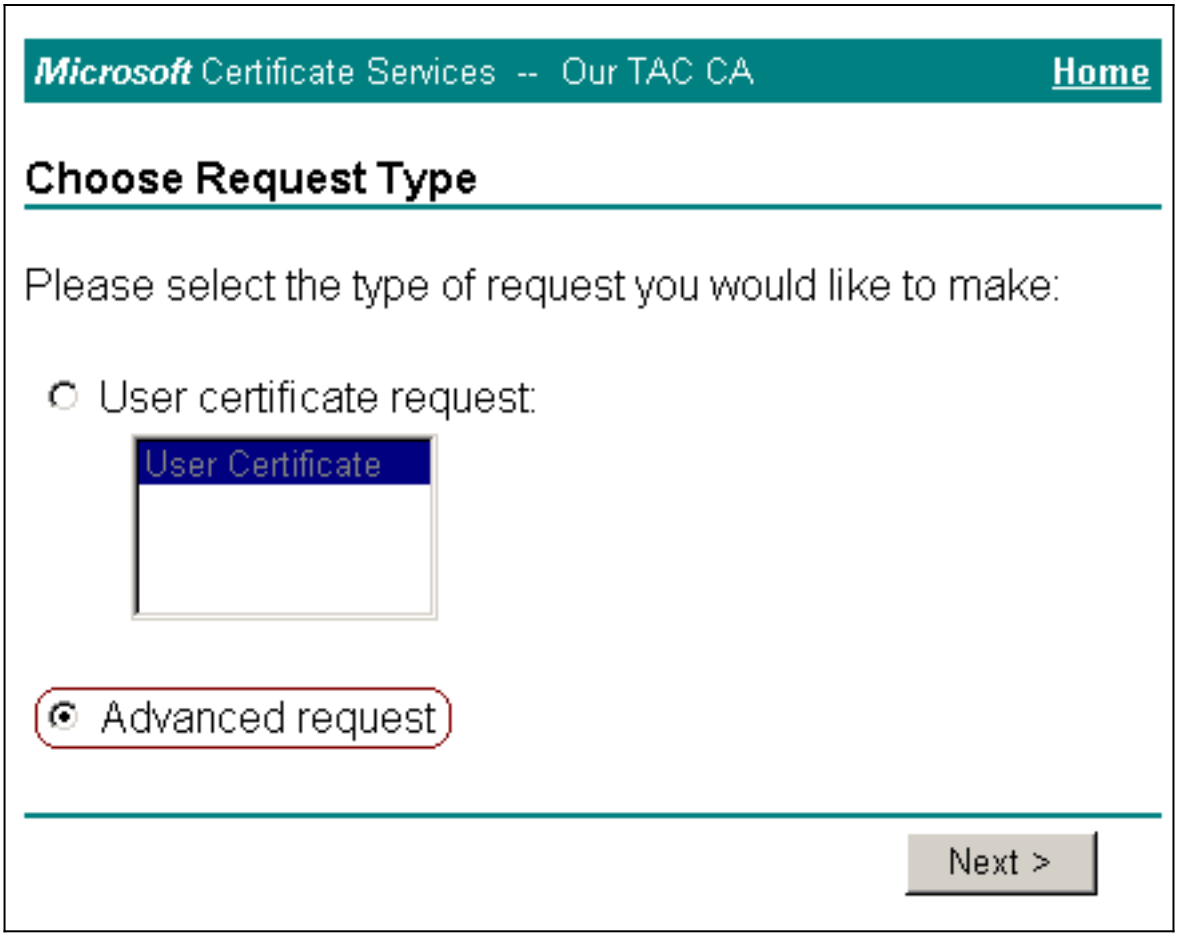
1. ACS サーバで Web ブラウザを開き、アドレス バーに http://CA-ip-address/certsrv と入力して CA サーバを表示します。 Administrator としてドメインにログインします。



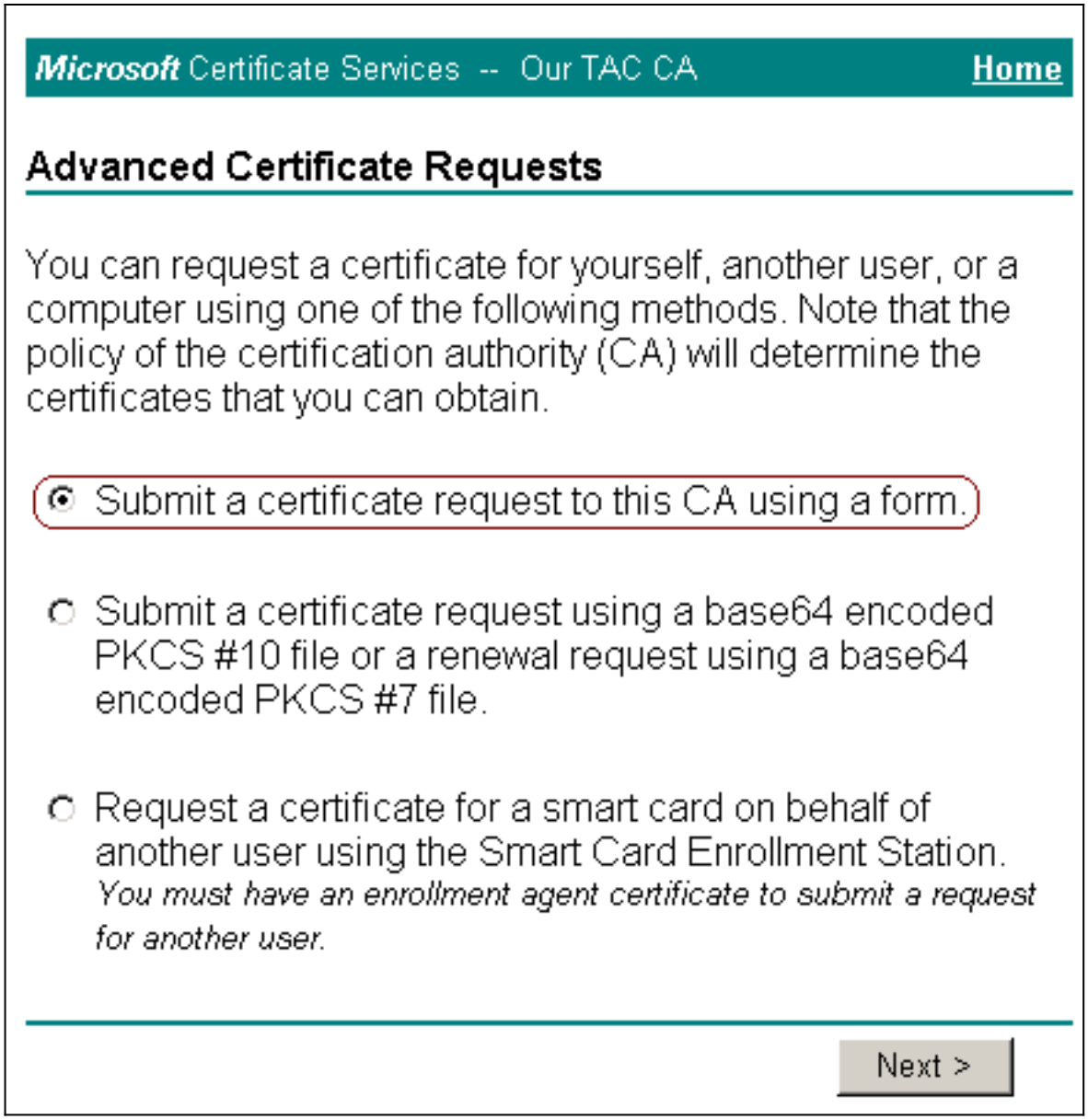
2. [Request a certificate] を選択してから [Next] をクリックします。



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

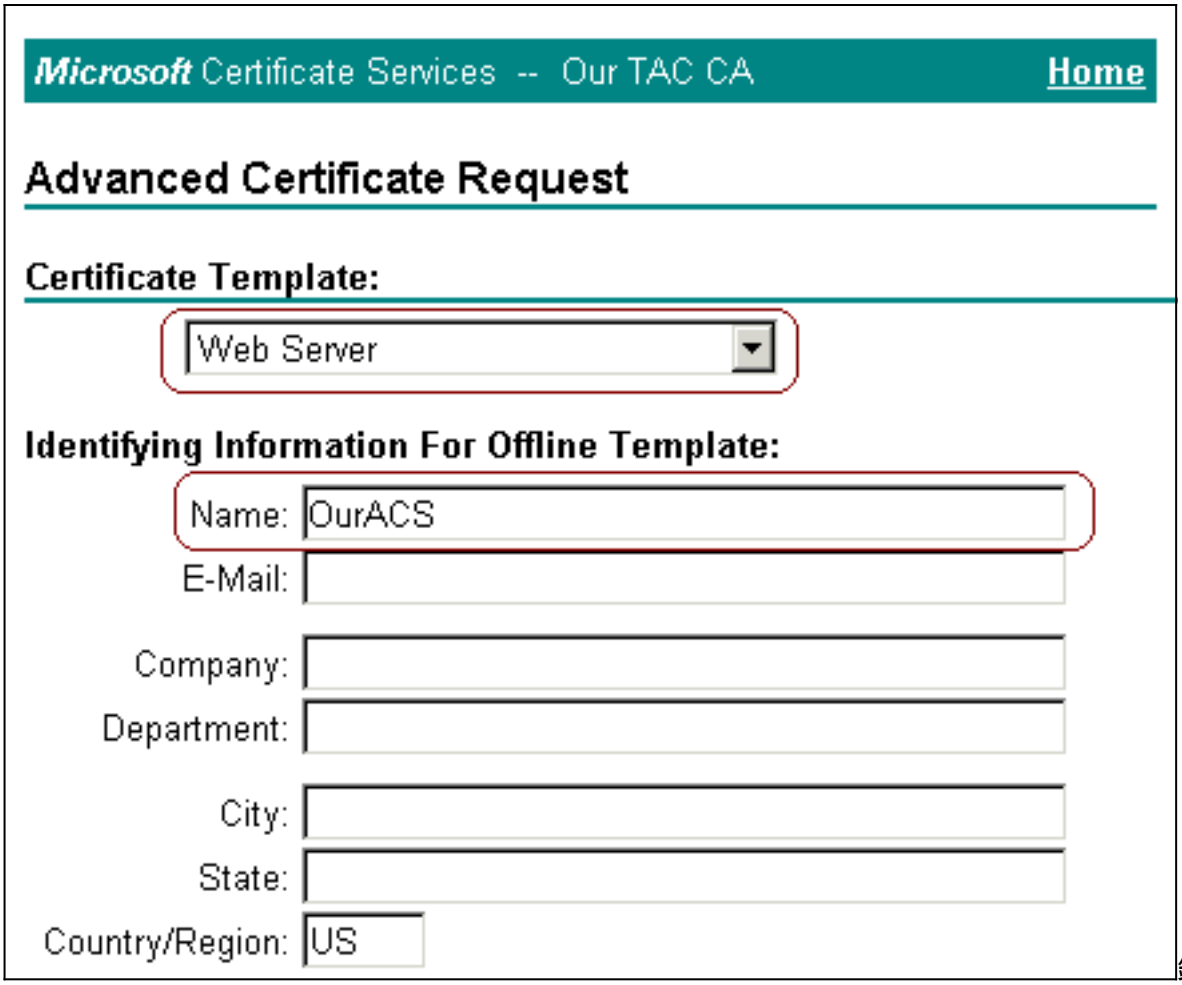


4. [Submit a certificate request to this CA using a form] を選択してから [Next] をクリックしま

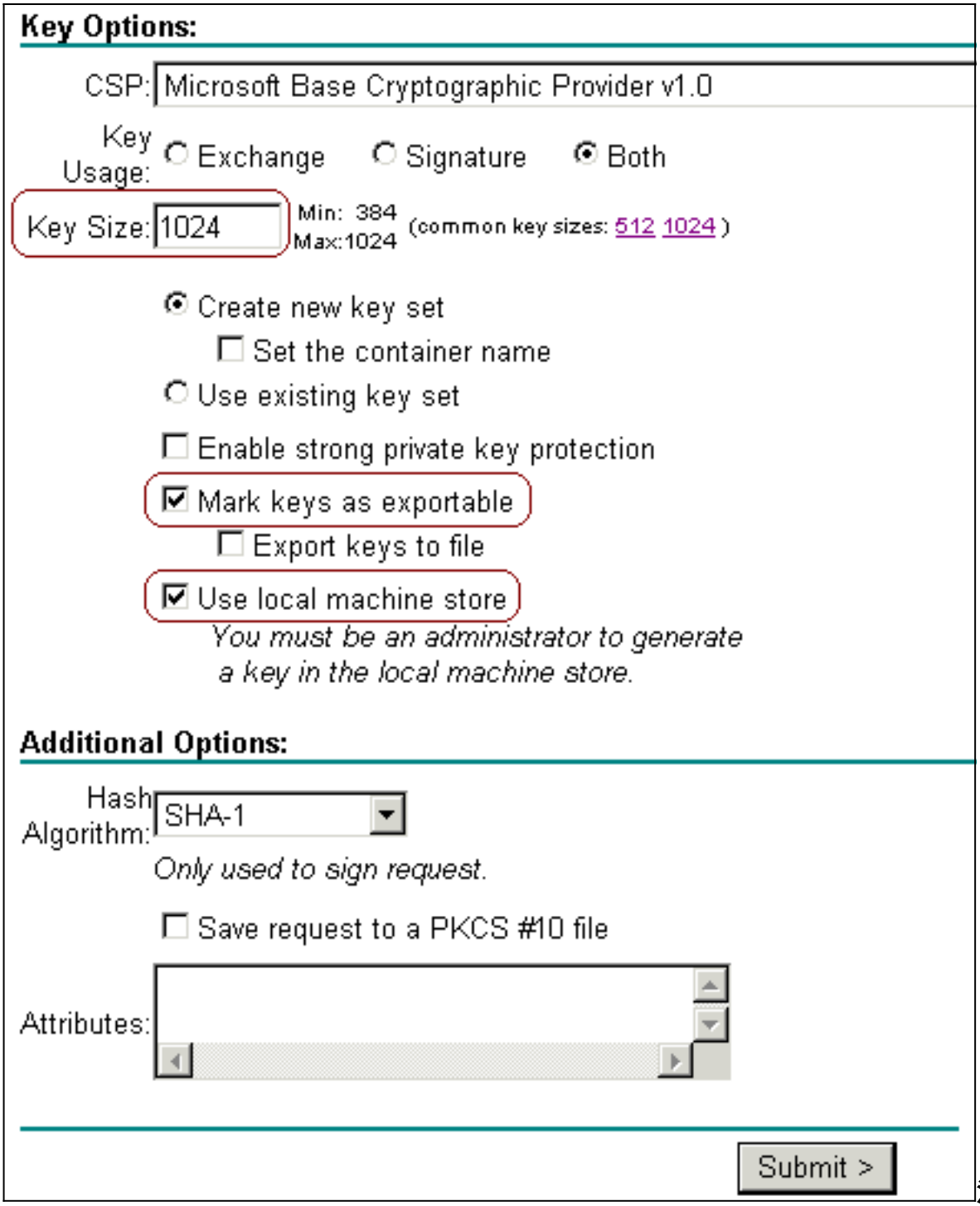


す。

5. 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 を選択します。 ACS サーバの名前を入力します。

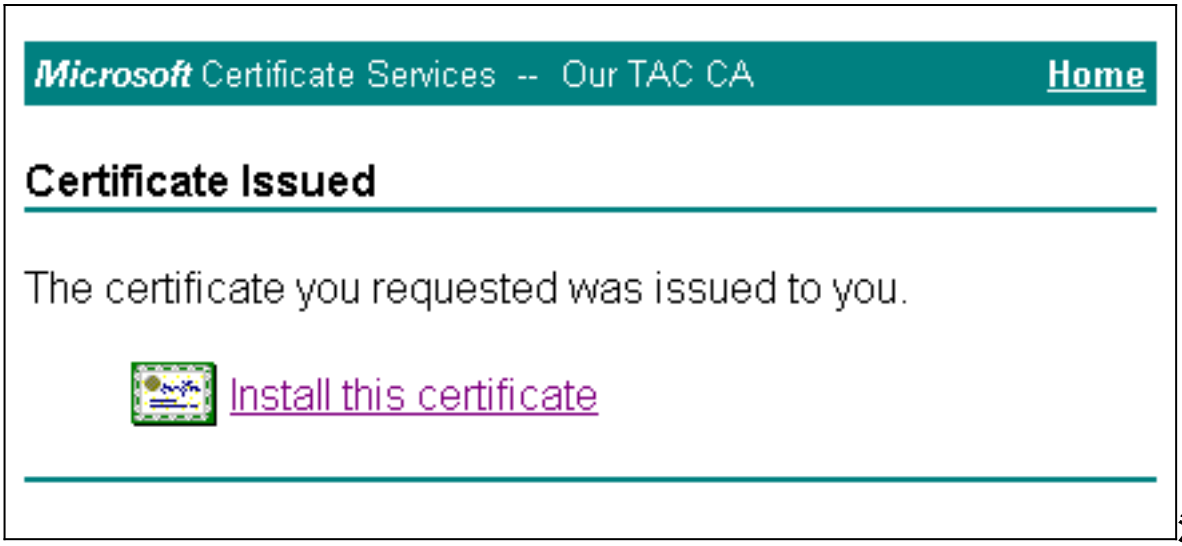


鍵のサイズを 1024 に設定します。 Mark keys as exportable と Use local machine store のオプションを選択します。 必要に応じてその他のオプションを設定し、[Submit] をクリックします。

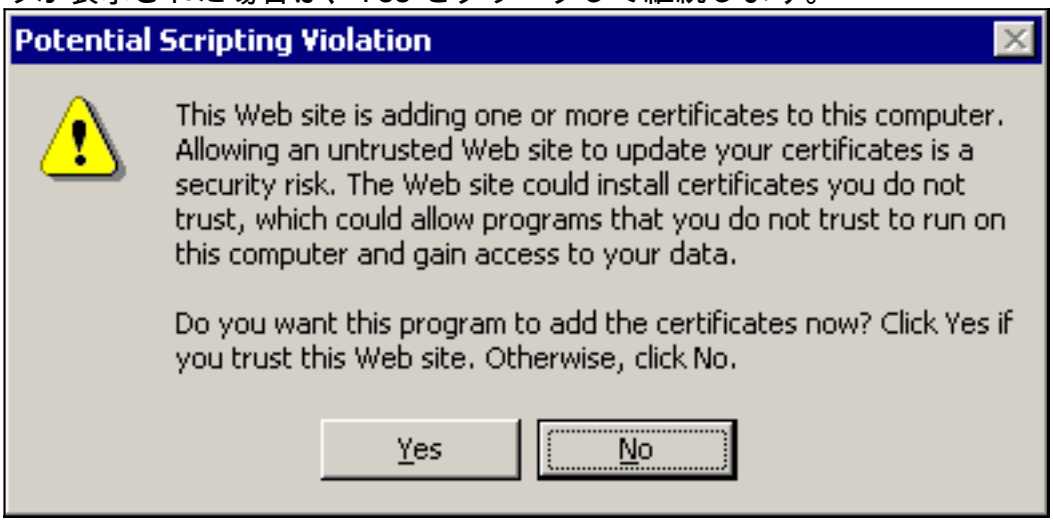


注:（ブラウザのセキュリティ/プライバシー設定に応じて）スクリプト違反を通知する警告ウィンドウが表示された場合は、Yes をクリックして継続します。

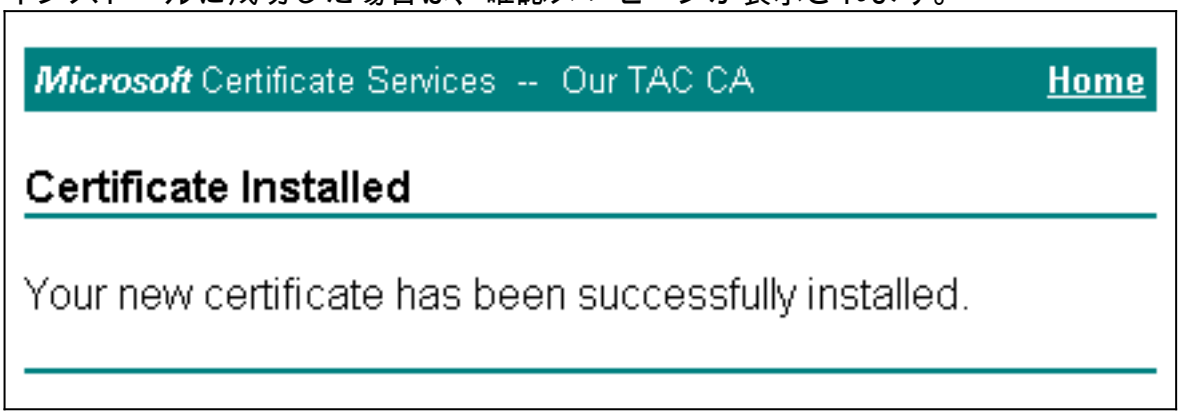
6. [Install this certificate] をクリックします。



注:（ブラウザのセキュリティ/プライバシー設定に応じて）スクリプト違反を通知する警告ウィンドウが表示された場合は、Yes をクリックして継続します。



7. インストールに成功した場合は、確認メッセージが表示されます。



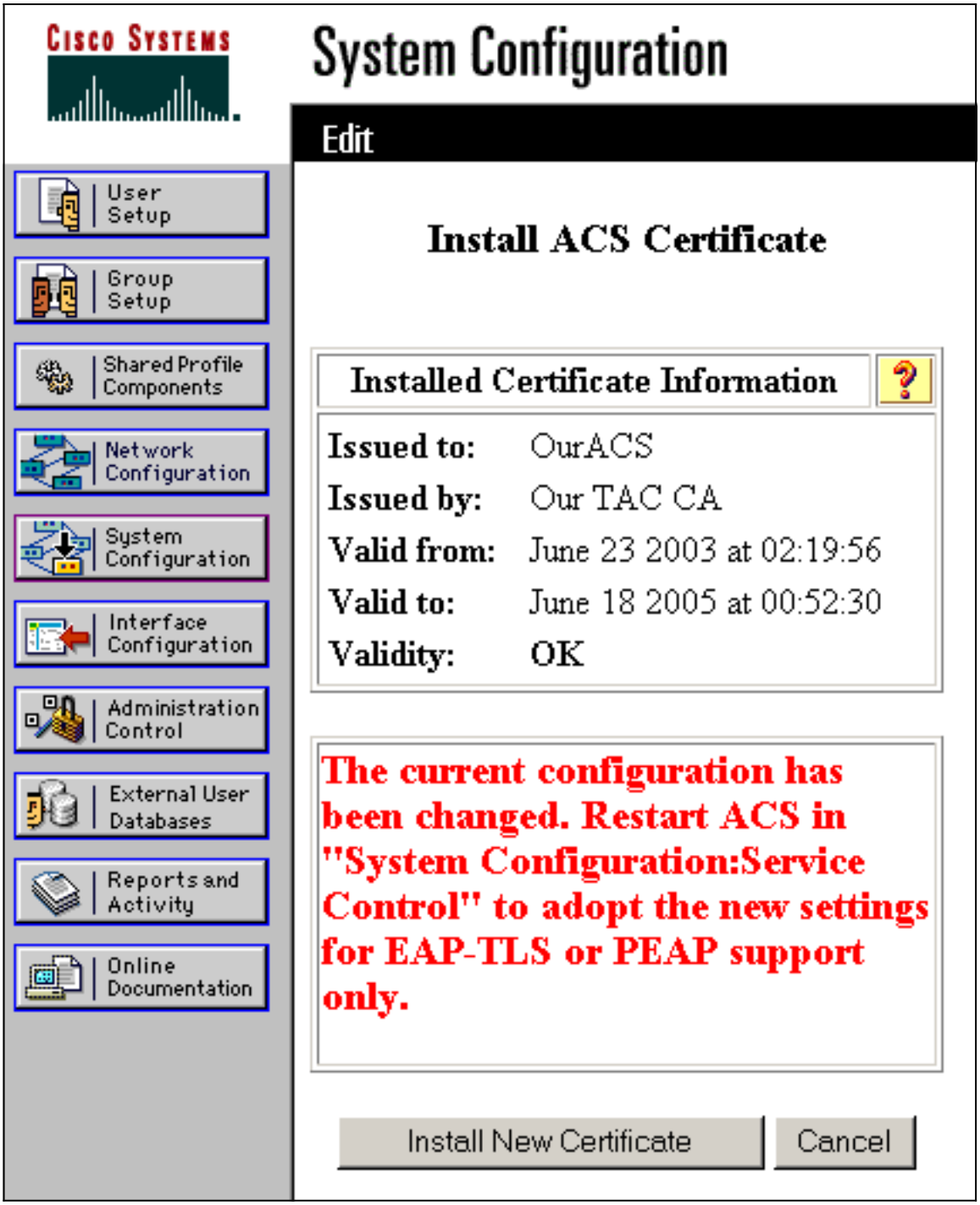
ストレージから証明書を使用するよう ACS を設定する

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、アドレス バーに http://ACS-ip-address:2002/ と入力して ACS サーバを表示します。 [System Configuration] をクリックし、[ACS Certificate Setup] をクリックします。
2. [Install ACS Certificate] をクリックします。
3. Use certificate from storage を選択します。 Certificate CN フィールドでは、セクションのステップ 5a で得る ACS サーバのための認証を割り当てた認証の名前を入力して下さい。

[Submit] をクリックします。ここで入力する情報は、高度な証明書の要求時に Name フィールドにタイプした名前と同じである必要があります。 それはサーバ証明の Subject フィールドの CN 名前です; この名前があるように確認するためにサーバ証明を編集できます。 この例では、この名前は「OurACS」です。 発行者の CN 名は入力しないでください。

4. 設定が完了すると、ACS サーバの設定が変更されたことを示す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、独自の証明書を発行した CA を自動的に信頼します。 クライアントの証明書が追加の 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。 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。

3. Edit Certificate Trust List をクリックします。 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。 [Submit] をクリックします。

サービスを再起動し、ACS での PEAP の設定を設定する

サービスを再開し、PEAP 設定を行うために次の手順に従って下さい。

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. PEAP の設定を設定するには、System Configuration をクリックしてから Global Authentication Setup をクリックします。
4. 次に示す 2 つの設定をチェックし、その他の設定をデフォルトのままにします。 必要に応じて、Enable Fast Reconnect などの追加設定を設定できます。 設定を終えたら [Submit] をクリックします。**Allow EAP-MSCHAPv2Allow MS-CHAP Version 2 Authentication注:** Fast Connect の詳細については、『システム設定： 認証と証明書』の「認証設定オプション」を参照してください。