用于Windows v3.2的安全ACS，带EAP-TLS计算机身份验证

目录

简介

本文档介绍如何使用Windows版本3.2的思科安全访问控制系统(ACS)配置可扩展身份验证协议传输层安全(EAP-TLS)。

注意：Novell证书颁发机构(CA)不支持计算机身份验证。ACS可以使用EAP-TLS支持对Microsoft Windows Active Directory进行计算机身份验证。最终用户客户端可能会将用于用户身份验证的协议限制为用于计算机身份验证的同一协议。也就是说，使用 EAP-TLS 进行计算机身份验证可能需要使用 EAP-TLS 进行用户身份验证。有关计算机身份验证的详细信息，请参阅 *Cisco 安全访问控制服务器 4.1 用户指南 中的*计算机身份验证部分。

注意：当设置ACS以通过EAP-TLS对计算机进行身份验证且已为计算机身份验证设置ACS时，必须

将客户端配置为仅执行计算机身份验证。有关详细信息，请参阅如何在Windows Vista、Windows Server 2008和Windows XP Service Pack 3中为基于802.1X的网络启用仅计算机身份验证。

先决条件

要求

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco Secure ACS for Windows v3.2
- Microsoft 证书服务（作为企业根证书颁发机构 [CA] 安装）**注意：**有关详细信息，请参阅设置认证机构的分步指南 。
- DNS 服务和 Windows 2000 Server（装有 Service Pack 3 和修补程序 323172）**注：如**果遇到CA服务器问题，请安装修补程序323172 。Windows 2000 SP3客户端需要修补程序 313664来启用IEEE 802.1x身份验证。
- Cisco Aironet 1200 系列无线接入点 12.01T
- 运行 Windows XP Professional（装有 Service Pack 1）的 IBM ThinkPad T30

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

背景理论

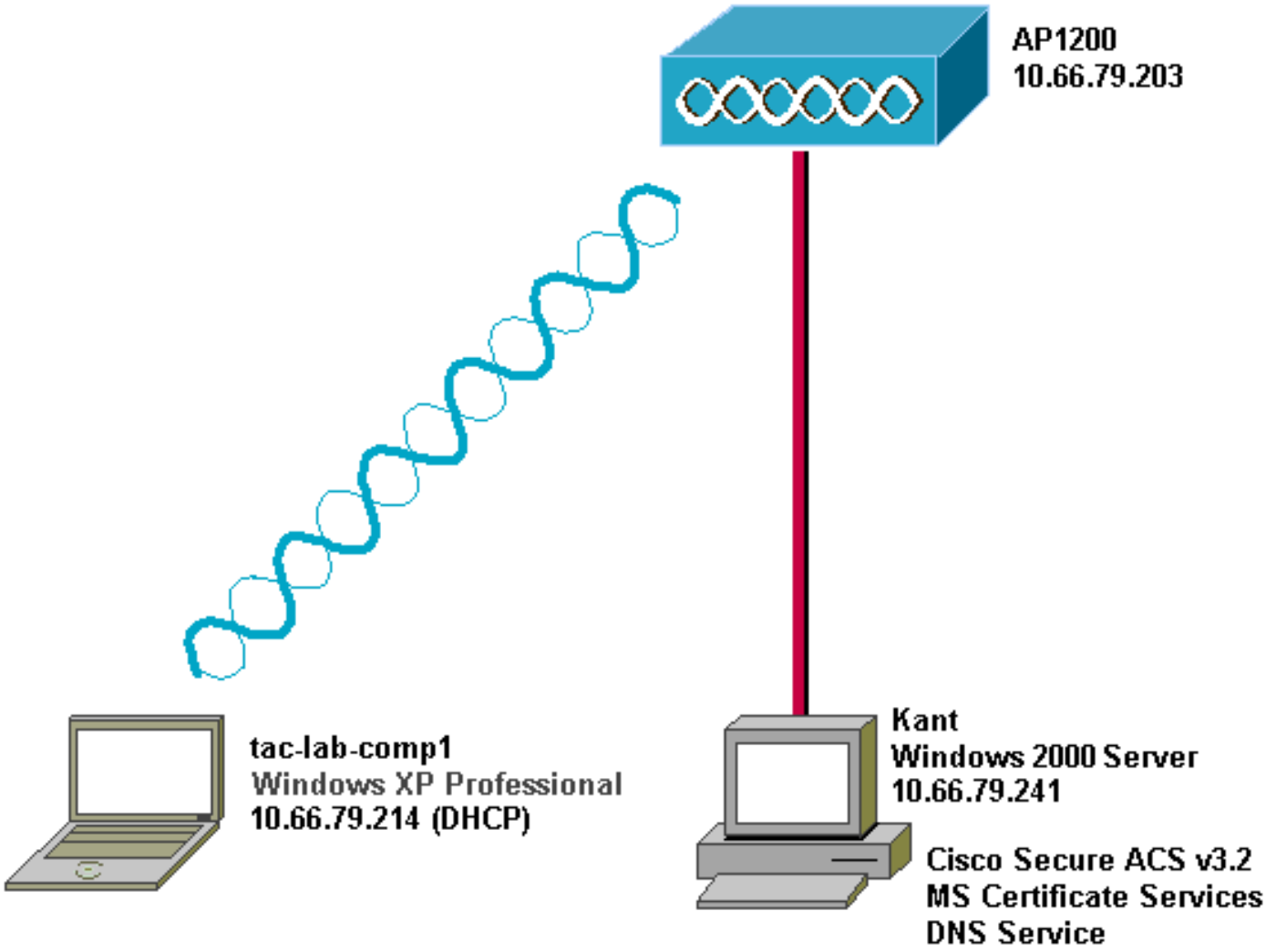
EAP-TLS和受保护可扩展的身份验证协议 (PEAP) 建立和使用TLS/Secure套接层(SSL)隧道。EAP-TLS 在 ACS 服务器（身份验证、授权和记帐 [AAA]）和客户端都有证书的情况下使用相互认证，证明它们彼此的身份。然而，PEAP 仅使用服务器端身份验证；只有服务器才具备证书，并向客户端证明其身份。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

网络图

本文档使用下图所示的网络设置。



配置 Cisco Secure ACS for Windows v3.2

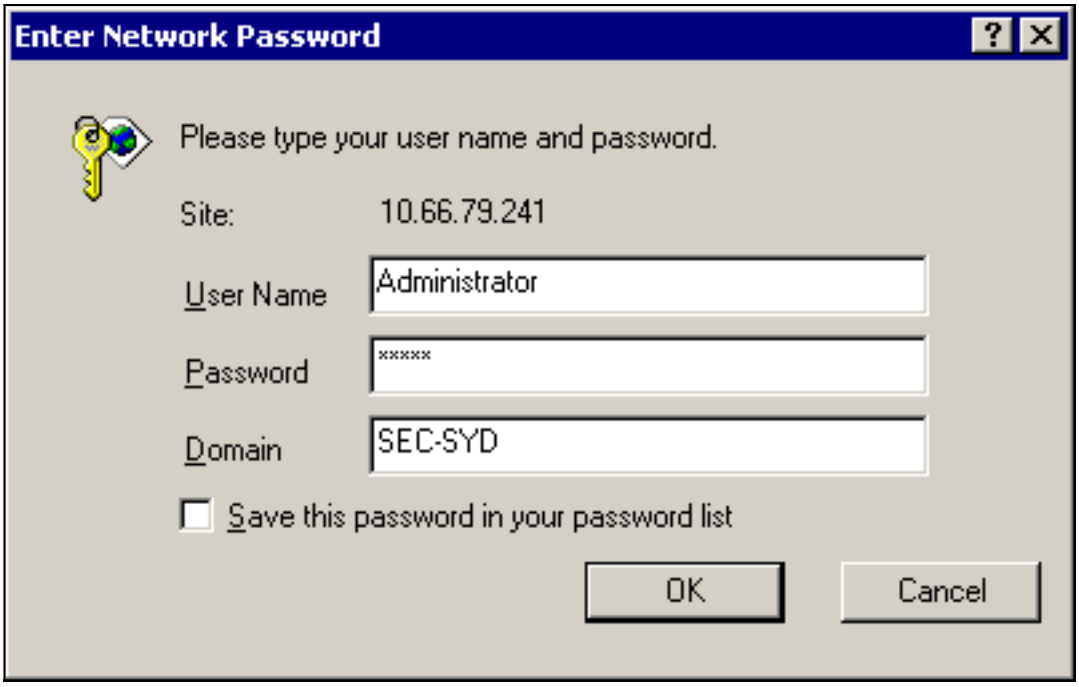
按照以下步骤配置 ACS 3.2。

1. 获取 ACS 服务器证书。
2. 配置 ACS 以使用存储中的证书。
3. 指定 ACS 应信任的其他证书颁发机构。
4. 重新启动服务并在 ACS 上配置 PEAP 设置。
5. 将接入点指定并配置为 AAA 客户端。
6. 配置外部用户数据库。
7. 重新启动服务。

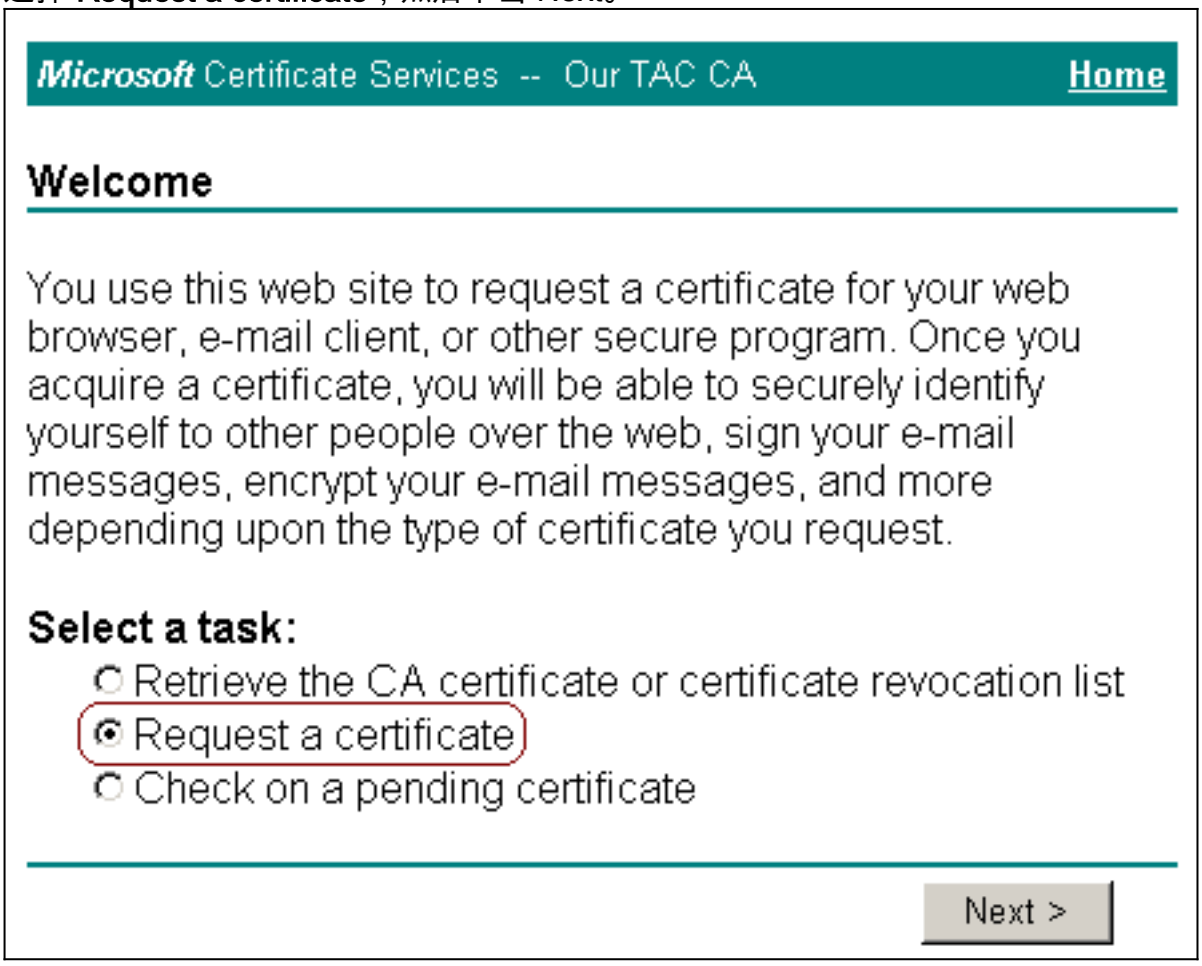
获取 ACS 服务器证书

按照以下步骤获取证书。

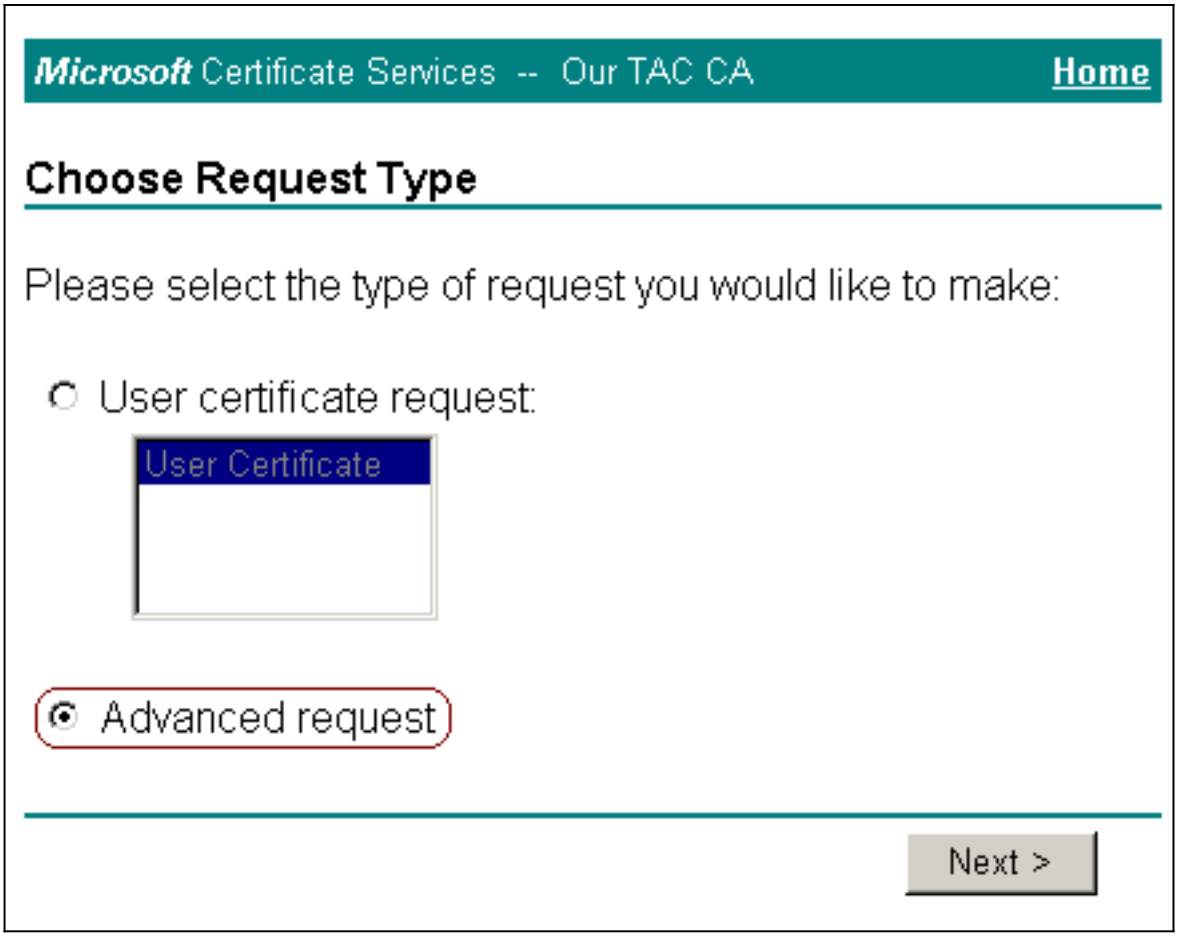
1. 在 ACS 服务器上打开 Web 浏览器，并输入 **http://CA-ip-address/certsrv 以便访问 CA 服务器**。
2. 以管理员身份登录到域。



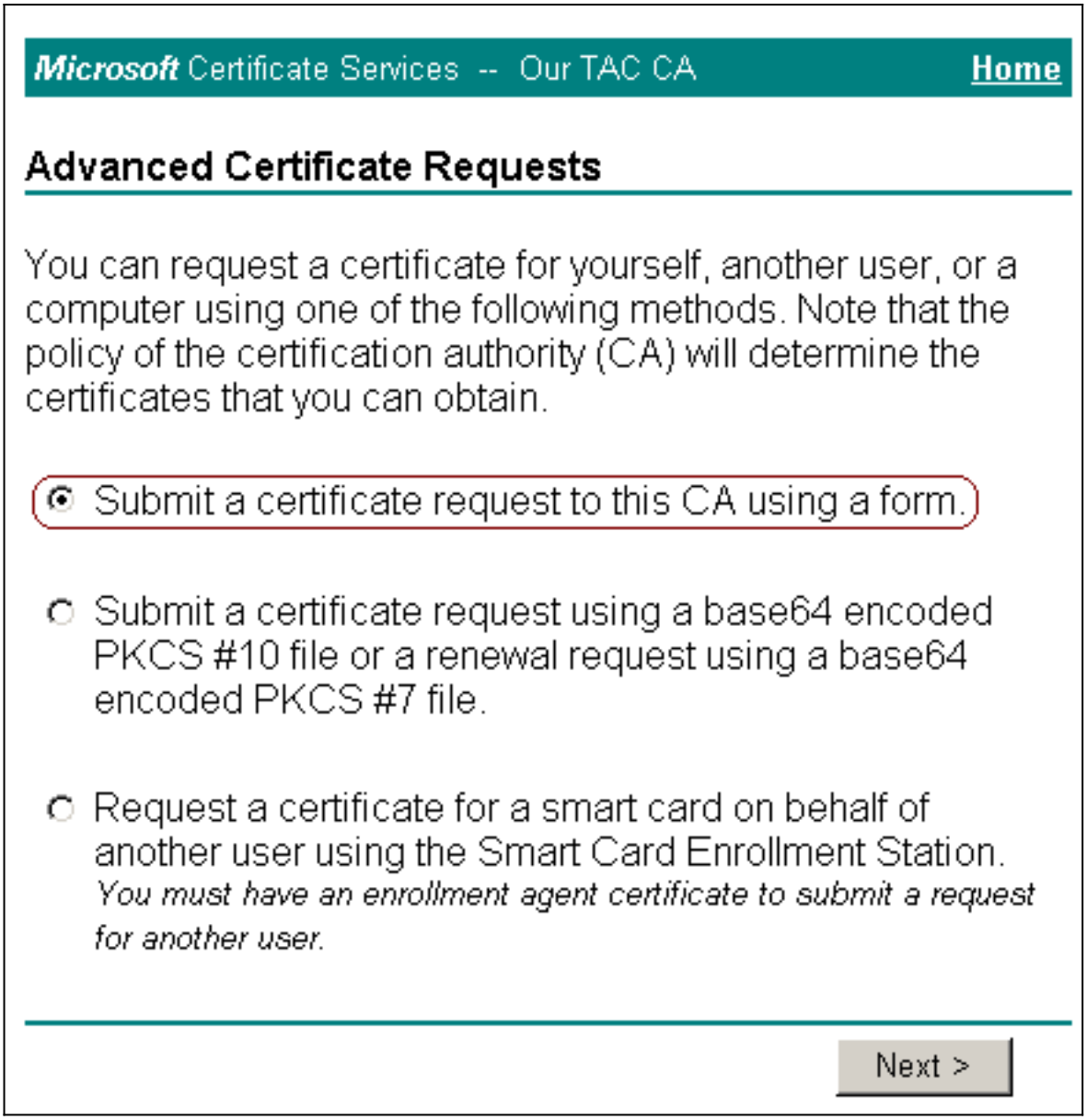
3. 选择 **Request a certificate**，然后单击 Next。



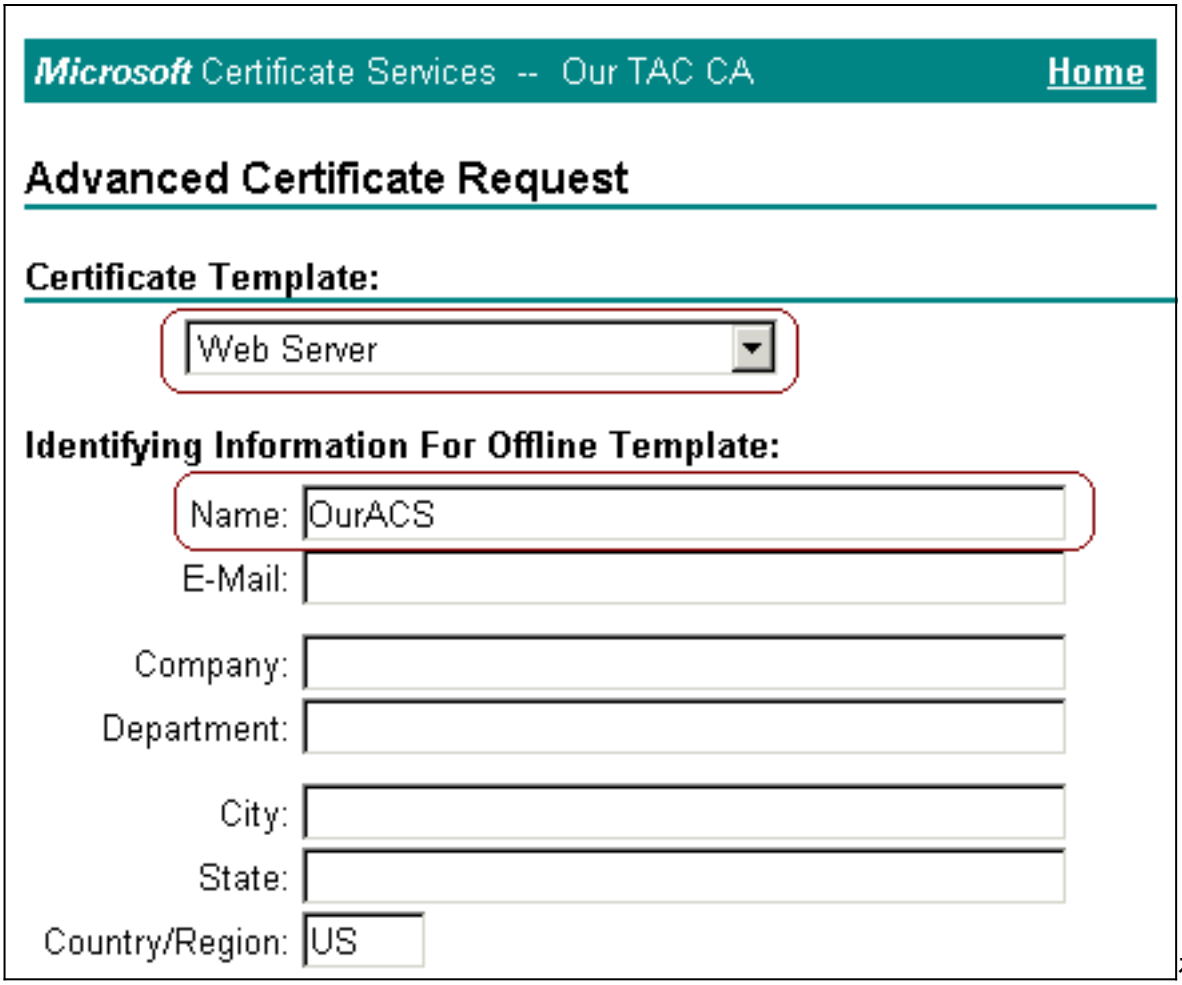
4. 选择 **Advanced request**，然后单击 Next。



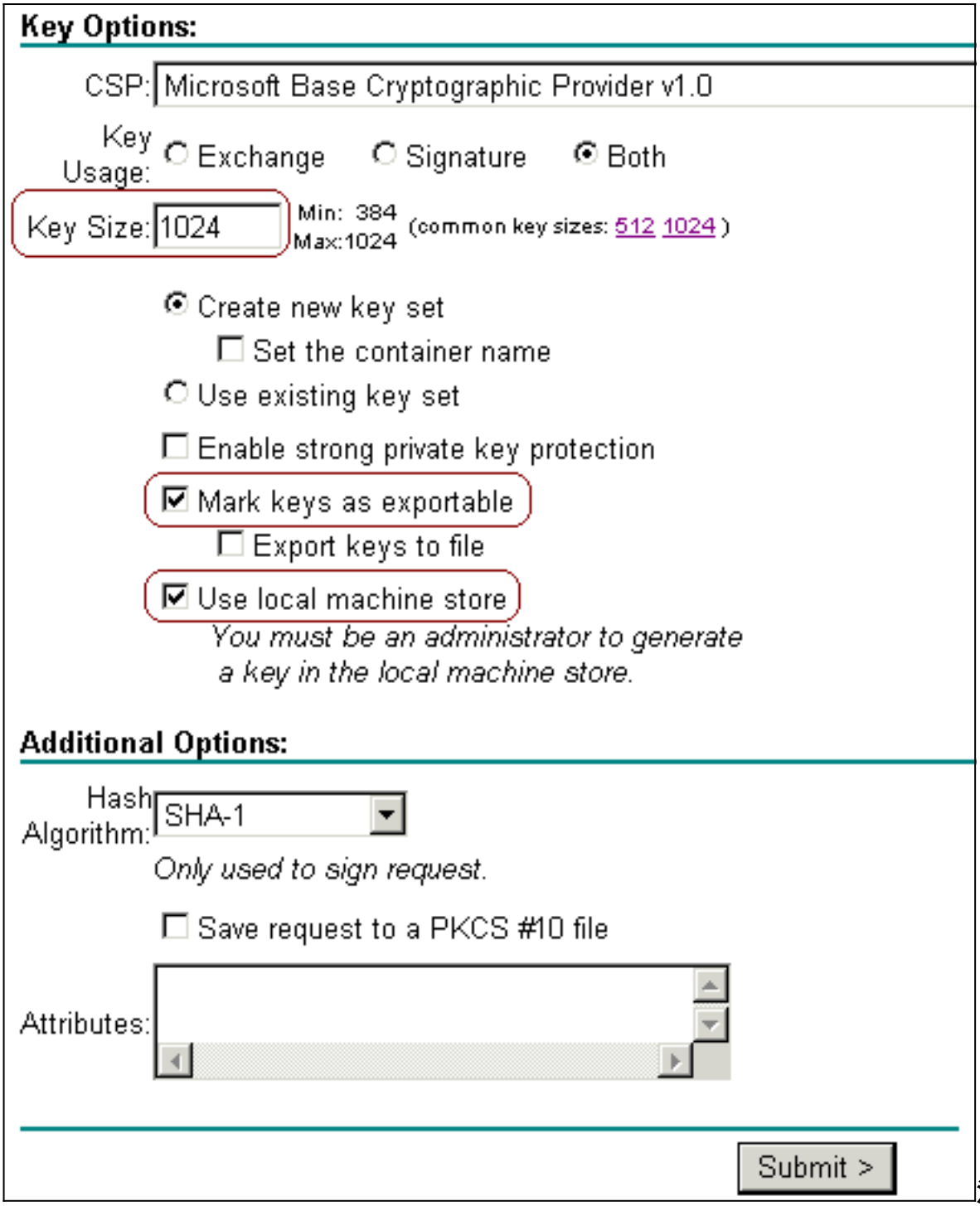
5. 选择 **Submit a certificate request to this CA using a form**，然后单击 Next。



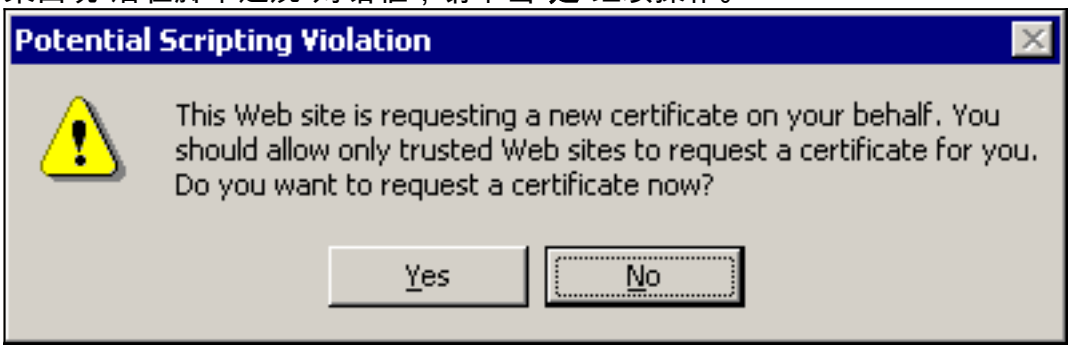
6. 配置证书选项：选择 **Web Server 作为证书模板，并输入 ACS 服务器的名称。**



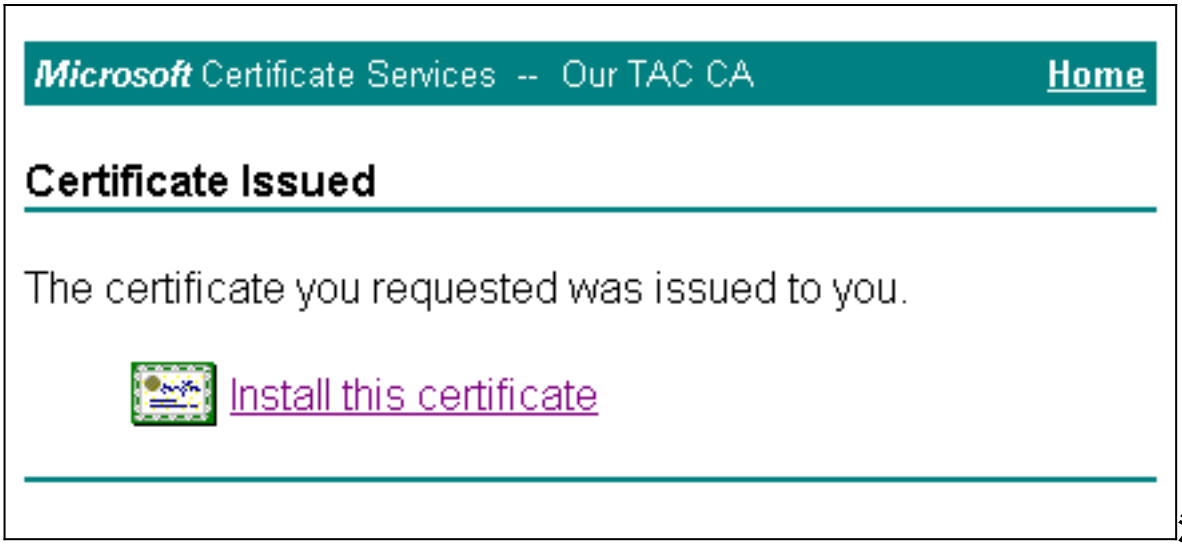
在 Key Size 字段中输入 **1024，并选中 Mark keys as exportable 和 Use local machine store 复选框**。根据需要配置其他选项，然后单击 **Submit**。



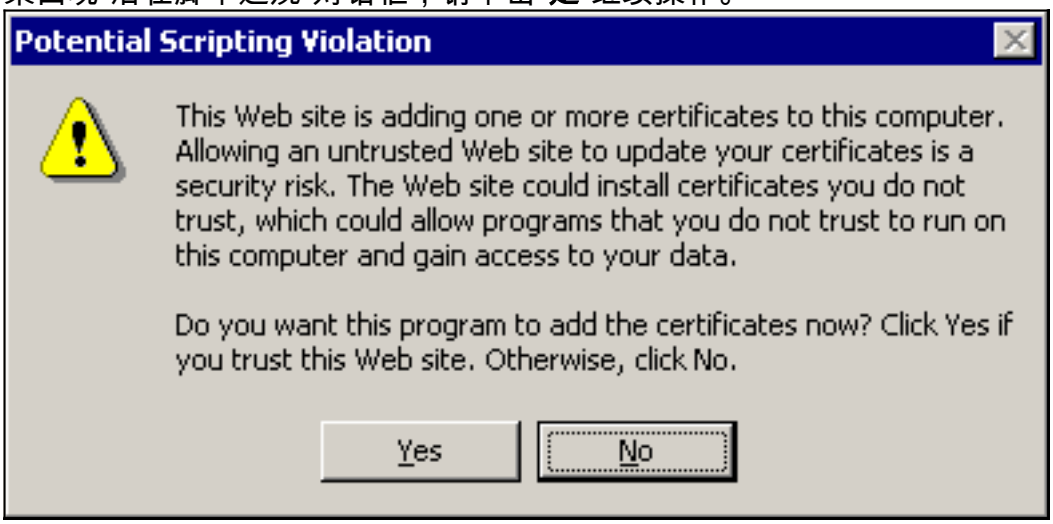
注意：如果出现“潜在脚本违规”对话框，请单击“**是**”继续操作。



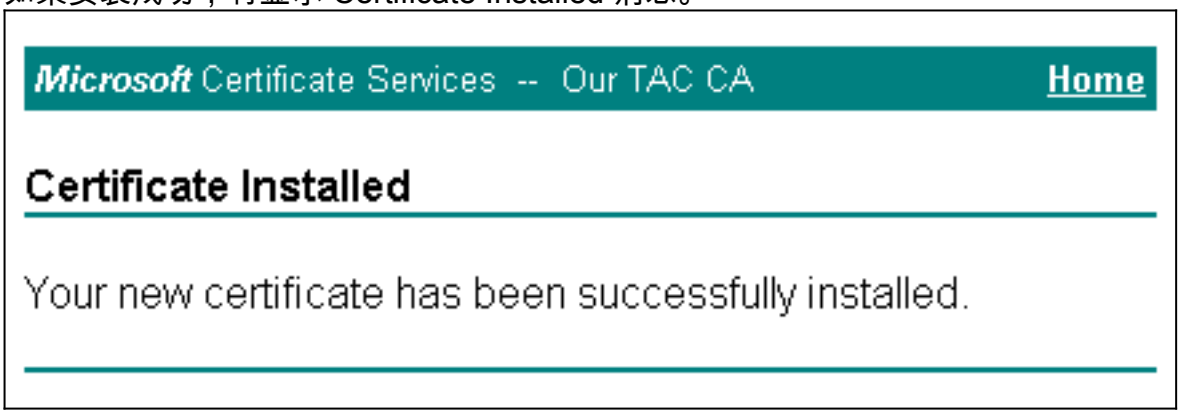
7. 单击 **Install this certificate**。



注意：如果出现“潜在脚本违规”对话框，请单击“**是**”继续操作。



8. 如果安装成功，将显示 Certificate Installed 消息。



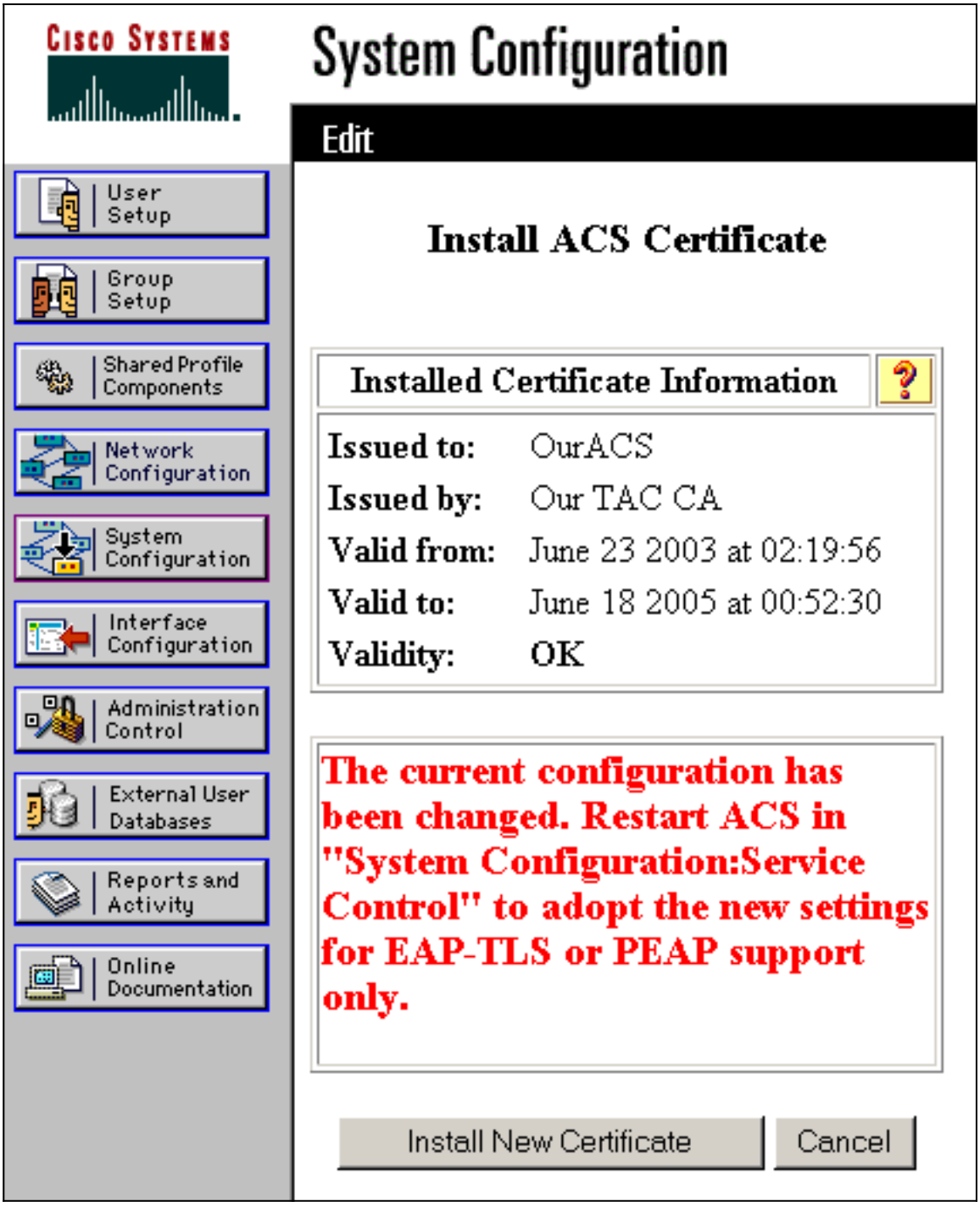
配置 ACS 以使用存储中的证书

请完成以下步骤以便将 ACS 配置为使用存储中的证书。

1. 打开 Web 浏览器，并输入 **http://ACS-ip-address:2002/ 以访问 ACS 服务器。**
2. 单击 **System Configuration**，然后单击 ACS Certificate Setup。
3. 单击 **Install ACS Certificate**。
4. 单击 **Use certificate from storage 单选按钮。**
5. 在 Certificate CN 字段中，输入您在本文档获取 ACS 服务器证书部分的步骤 5a 中指定的证书名称。
6. 单击“Submit”。

配置完成之后，将显示一条确认消息，指示 ACS 服务器配置已发生更改。**注意**：此时您无需重新启动

ACS。



指定 ACS 应信任的其他证书颁发机构

ACS 自动信任颁发其自己的证书的 CA。如果客户端证书由其他 CA 颁发，您必须完成以下步骤：

1. 单击 **System Configuration**，然后单击 ACS Certificate Setup。
2. 单击 **ACS Certificate Authority Setup 以向受信任的证书列表添加 CA。**
3. 在 CA 证书文件的字段中，输入证书的位置，然后单击 **Submit。**

4. 单击 **Edit Certificate Trust List**。
5. 选中 ACS 应该信任的所有 CA，不要选择 ACS 不应信任的所有 CA。
6. 单击“Submit”。

重新启动服务并在 ACS 上配置 EAP-TLS 设置

完成以下步骤，以便重新启动服务和配置 EAP-TLS 设置：

1. 单击 **System Configuration**，然后单击 Service Control。
2. 单击 **Restart 以重新启动服务。**
3. 要配置 EAP-TLS 设置，请单击 **System Configuration**，然后单击 Global Authentication Setup。
4. 选中 **Allow EAP-TLS**，然后选中一个或多个证书比较。
5. 单击“Submit”。