配置Windows的v3.2 Cisco Secure ACS使用PEAP-MS-CHAPv2机器认证

Contents

Introduction

本文档演示如何使用针对 Windows 版本 3.2 的 Cisco Secure ACS 来配置受保护的可扩展的认证协议 (PEAP)。

使用无线局域网控制器，关于如何配置安全的无线访问的更多信息，微软视窗2003软件和思科安全访问控制服务器(ACS) 4.0，是指PEAP在与ACS 4.0和Windows 2003的统一的无线网络下。

Prerequisites

Requirements

本文档没有任何特定的前提条件。

Components Used

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）**Note:** 有关详细信息，请参阅证书颁发机构设置分步指南 。
- DNS 服务和 Windows 2000 Server（装有 Service Pack 3）**Note:** 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 才能启用 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。All of the devices used in this document started with a cleared (default) configuration.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

PEAP 和 EAP-TLS 构建并使用 TLS/安全套接字层 (SSL) 隧道。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。EAP-TLS，然而，使用ACS的相互验证(认证、授权和记帐[AAA])服务器和客户端有证书并且彼此证明他们的身份。

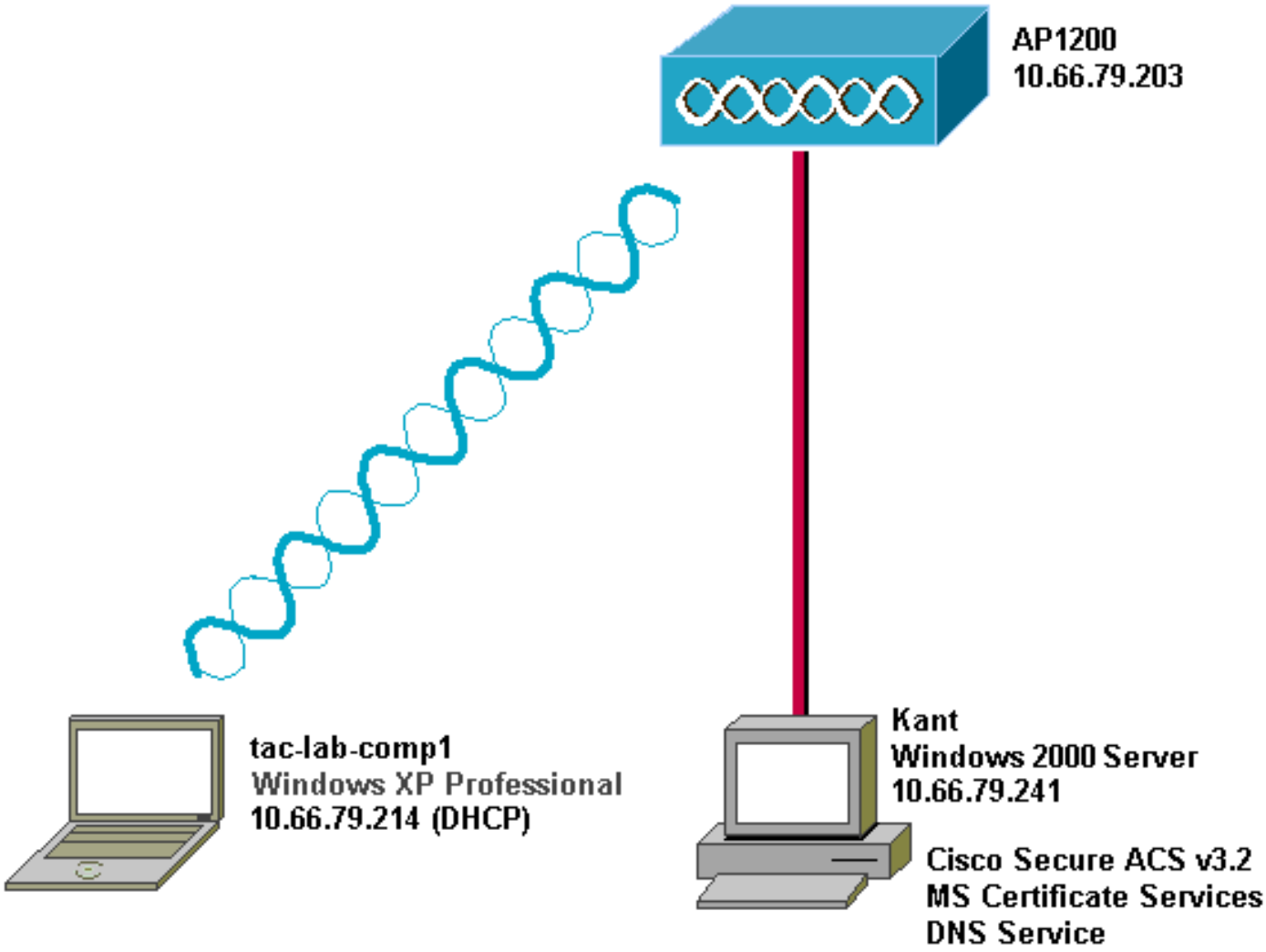
因为客户端不需要证书，因此 PEAP 非常方便。EAP-TLS 用于验证无外设设备，因为证书不需要任何用户交互。

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Network Diagram

本文档使用下图所示的网络设置。



配置 Cisco Secure ACS for Windows v3.2

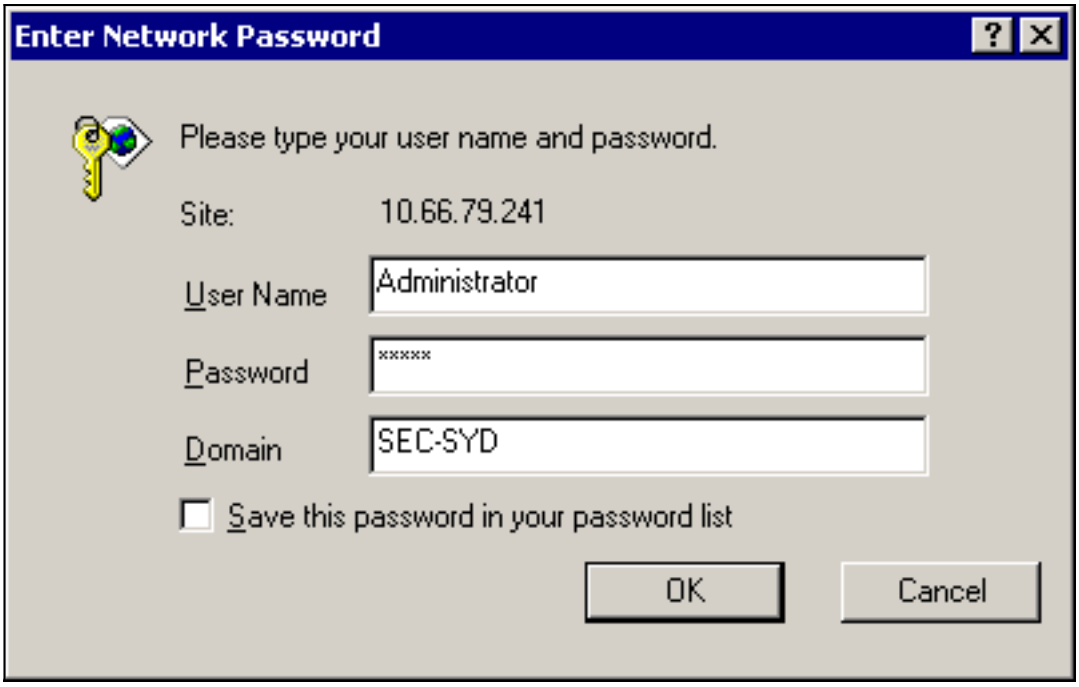
按照以下步骤配置 ACS 3.2。

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。

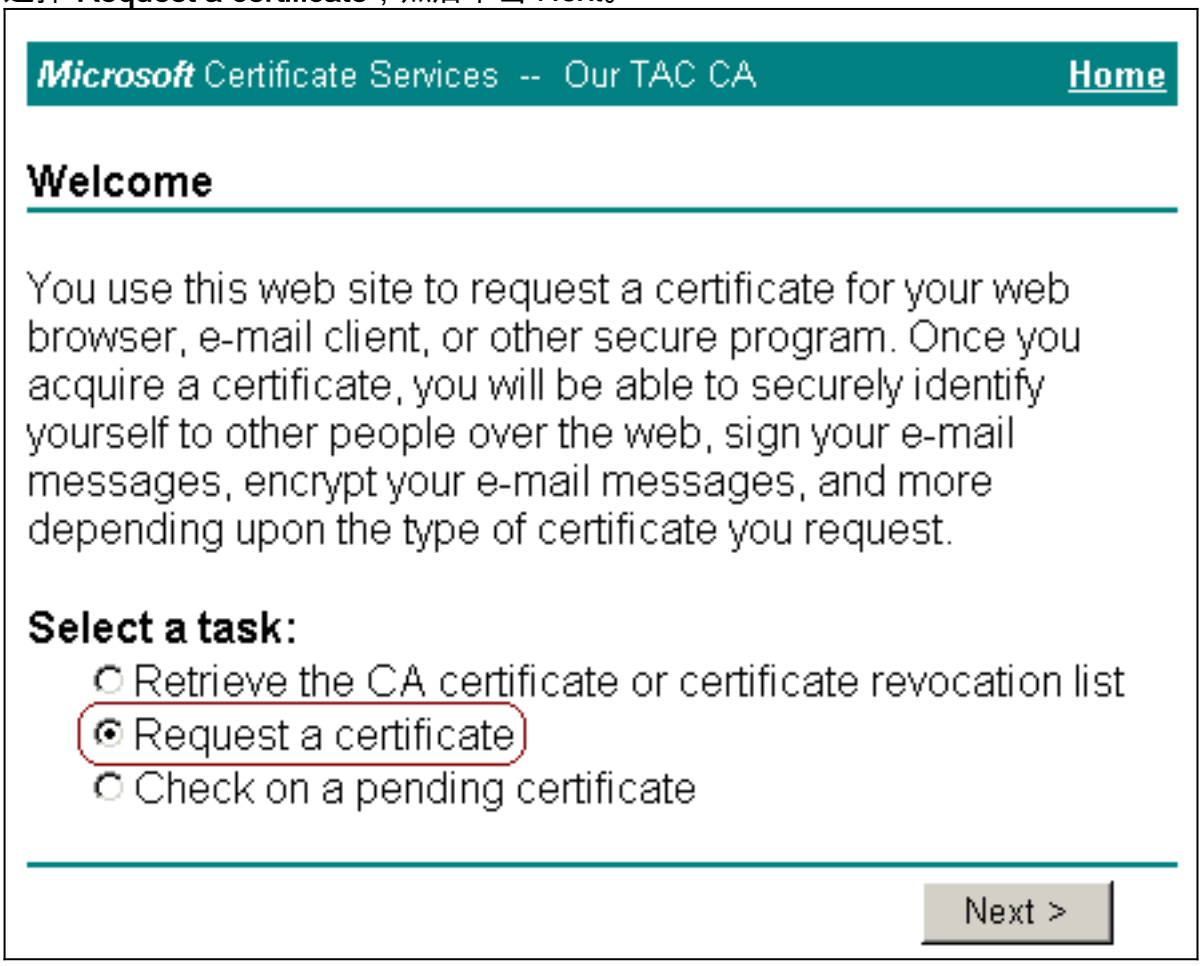
获取 ACS 服务器证书

按照以下步骤获取证书。

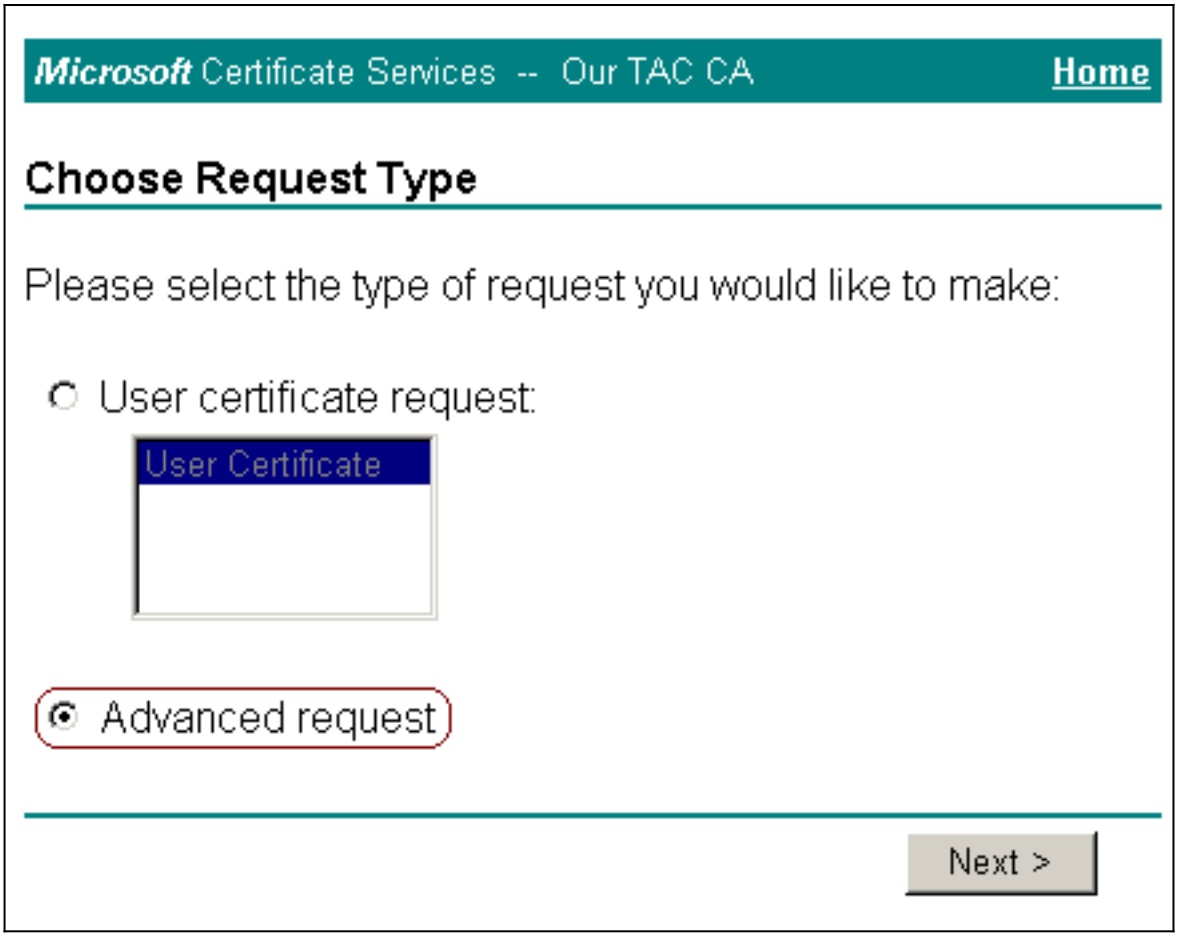
1. 在ACS服务器上，请打开Web浏览器并且访问到CA服务器通过输入**http:// CA IP*地址*/certsrv**在地址栏。以管理员身份登录到域。



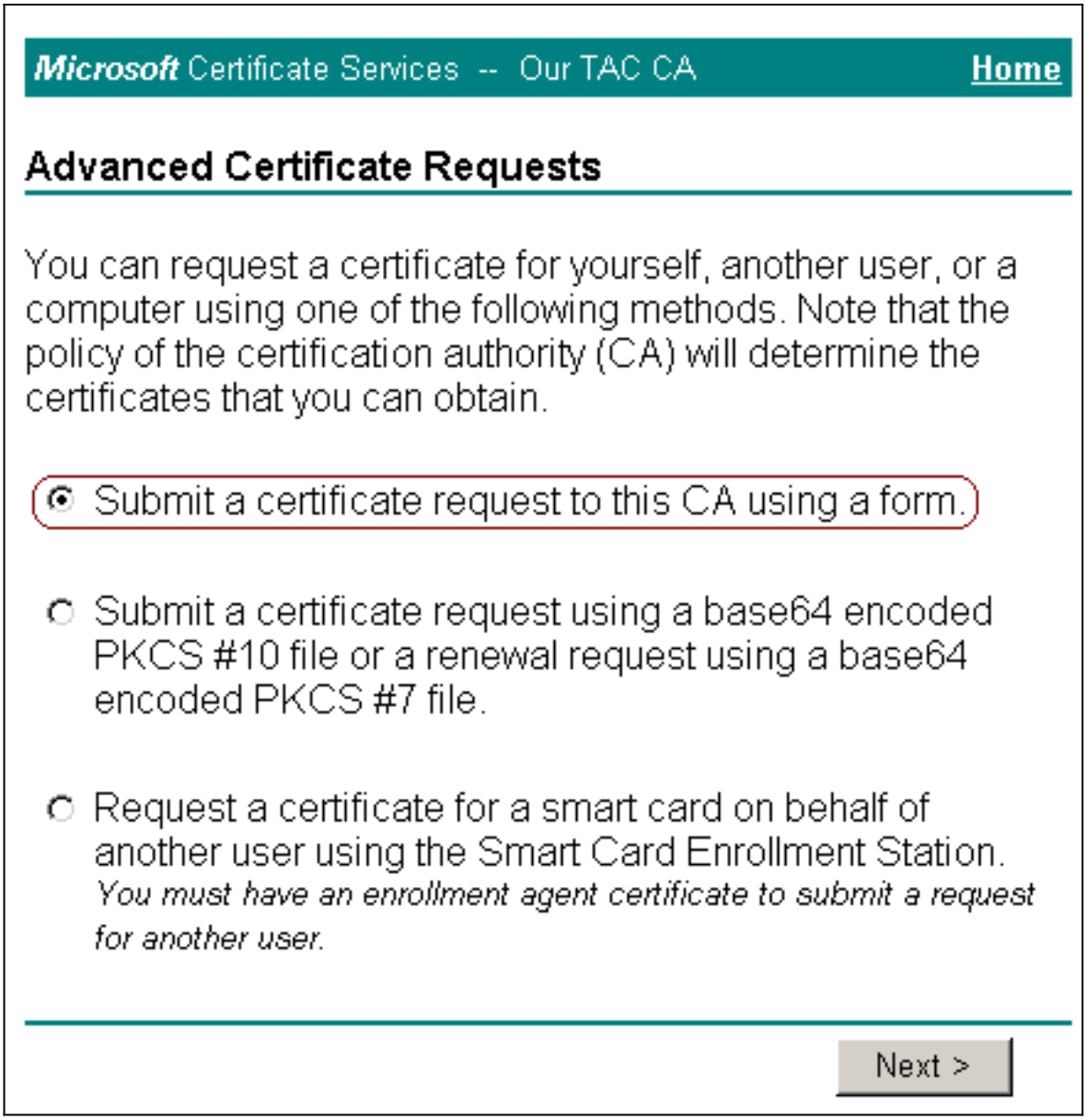
2. 选择 **Request a certificate**，然后单击 Next。



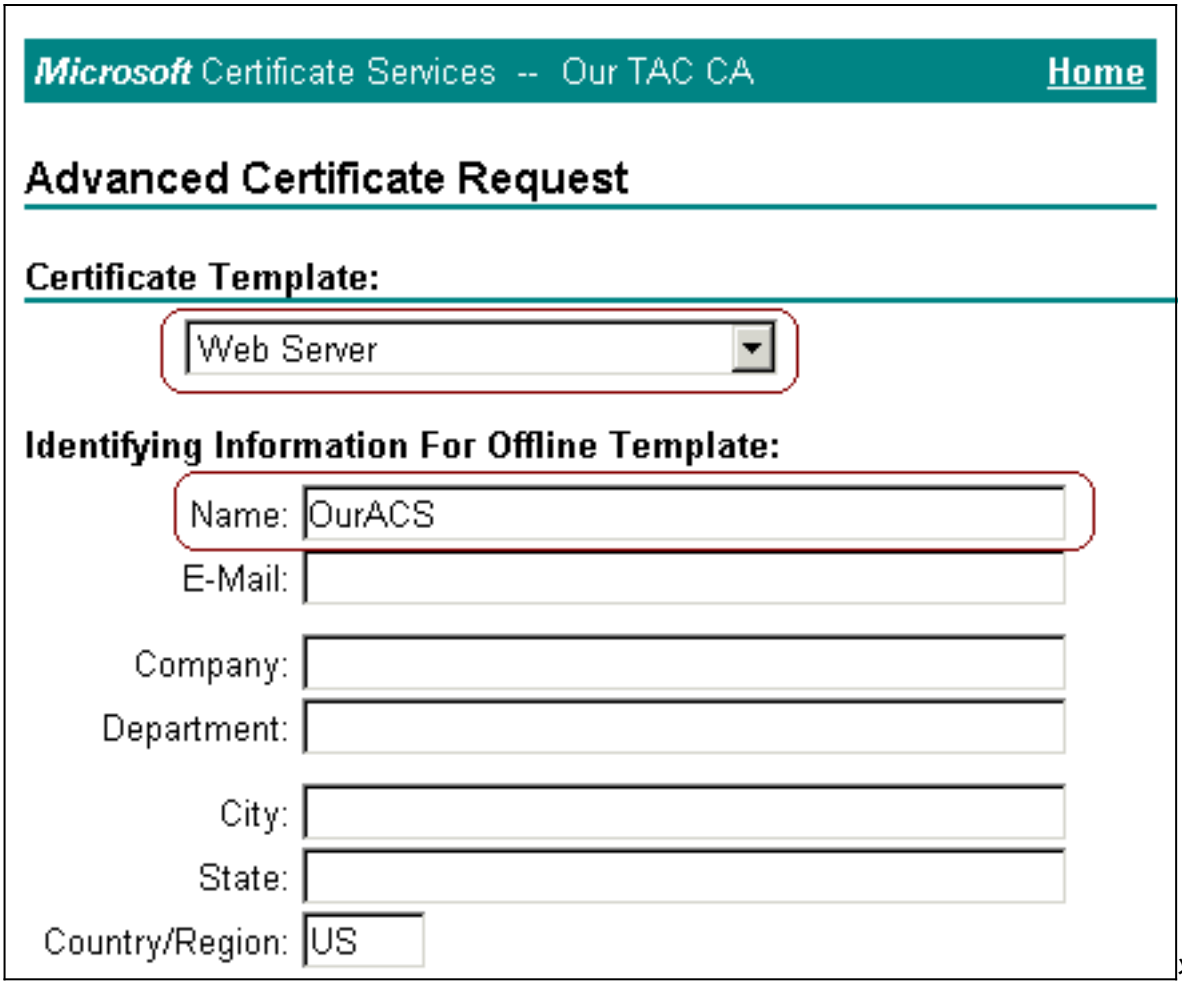
3. 选择 **Advanced request**，然后单击 Next。



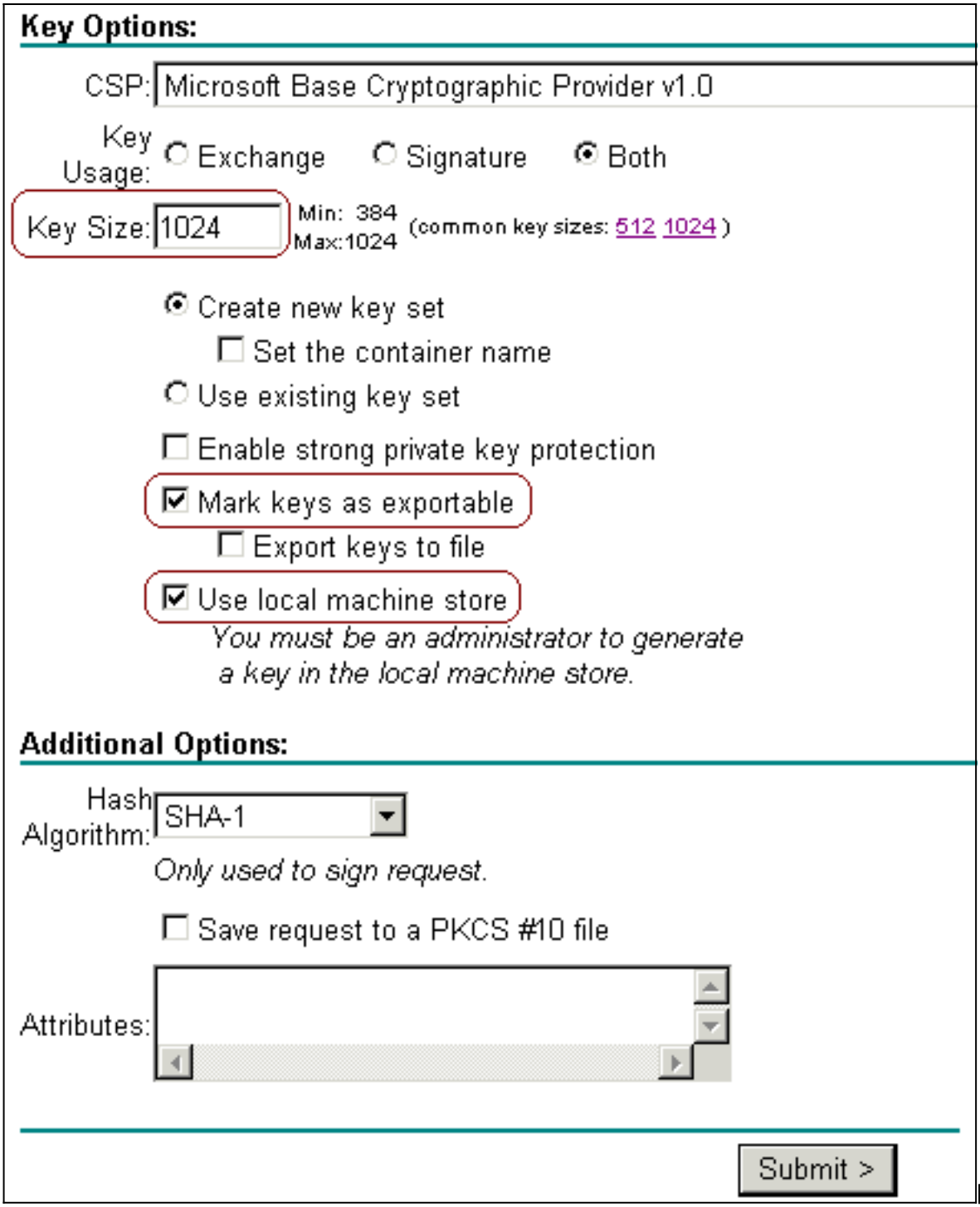
4. 选择 **Submit a certificate request to this CA using a form**，然后单击 Next。



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

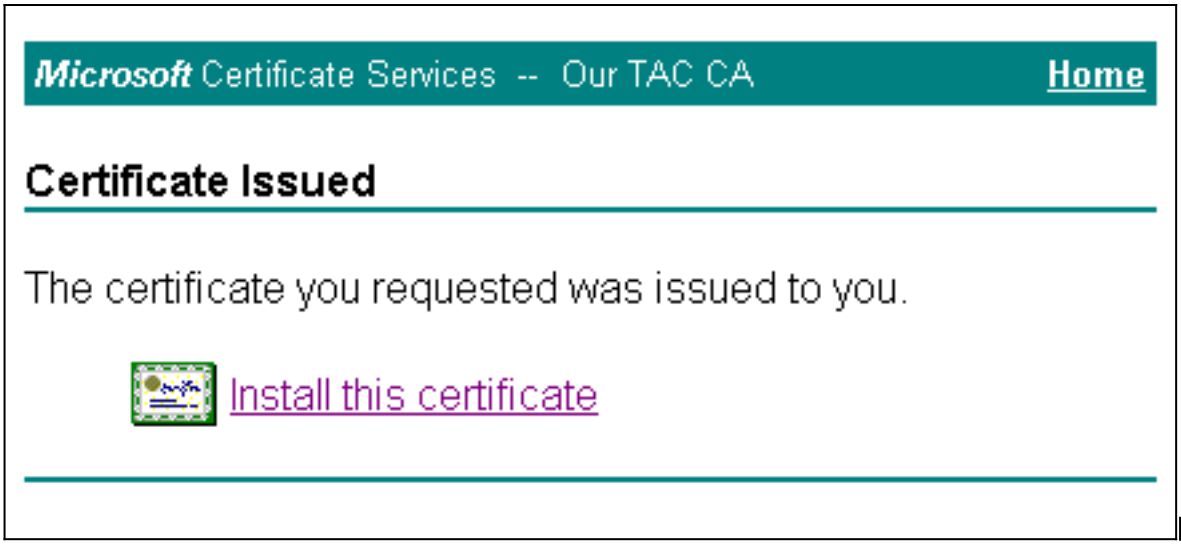


将密钥大小设置为 **1024**。选中 **Mark keys as exportable** 和 Use local machine store 选项。根据需要配置其他选项，然后单击 **Submit**。

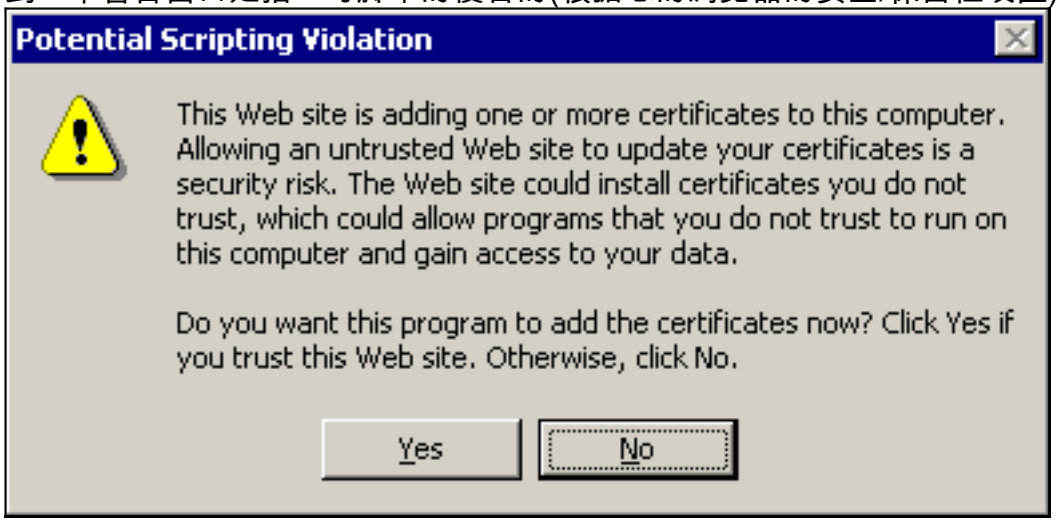


Note: 如果看到一个警告窗口是指一写脚本的侵害的(根据您的浏览器的安全/保密性设置)，**是请**点击继续。

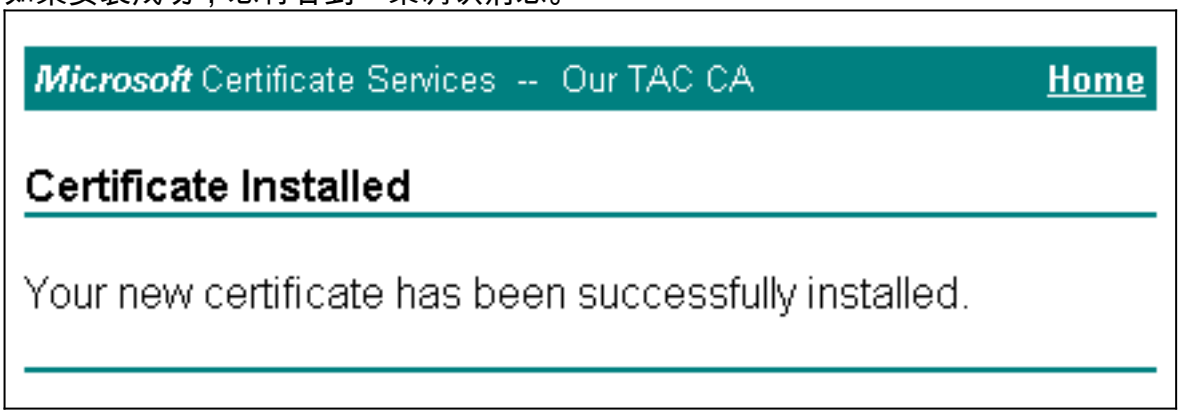
6. 单击 **Install this certificate**。



Note: 如果看到一个警告窗口是指一写脚本的侵害的(根据您的浏览器的安全/保密性设置)，**是请**点击继续。



7. 如果安装成功，您将看到一条确认消息。



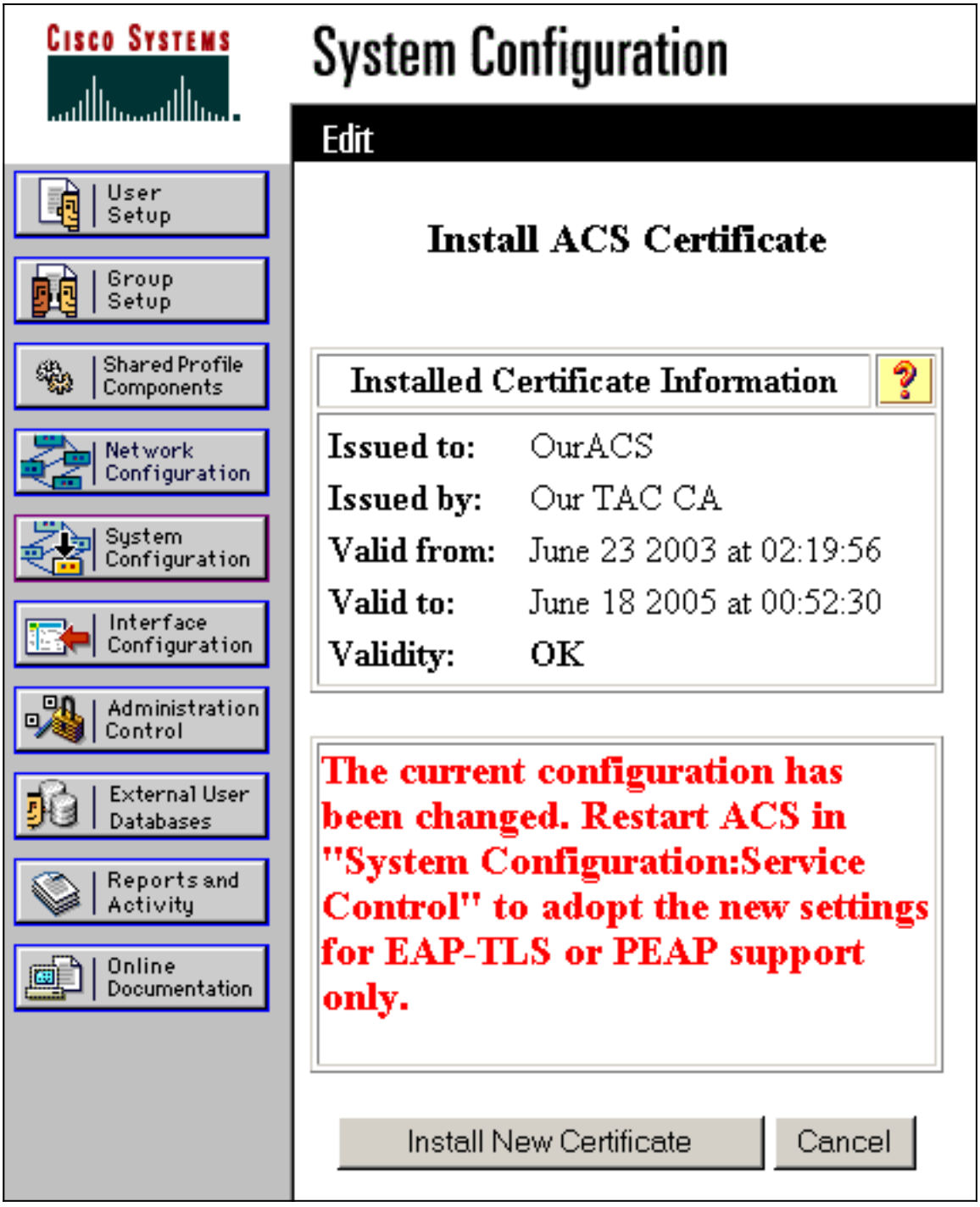
配置 ACS 以使用存储中的证书

按照以下步骤将 ACS 配置为使用存储中的证书。

1. 打开Web浏览器并且访问到ACS服务器通过输入**http:// ACS *IPaddress:2002/***在地址栏。单击 **System Configuration**，然后单击 ACS Certificate Setup。
2. 单击 **Install ACS Certificate**。
3. 选择 **Use certificate from storage**。在 Certificate CN 字段中，输入您在获取 ACS 服务器证书部分的步骤 5a 中指定的证书名称。单击 **submit**。此条目必须匹配在先进的证书请求期间，您输入名称字段的名字。该名称是服务器证书的 subject 字段中的 CN 名称；可以对服务器证书进行编辑，以查看此名称。在本示例中，该名称为“OurACS”。请 *勿* 输入颁发者的 CN 名称。

4. 当配置完成，您将看到确认消息表明更改了ACS服务器的配置。**Note:** 此时无需重新启动

ACS。



指定 ACS 应信任的其他证书颁发机构

ACS 将自动信任颁发其自己的证书的 CA。如果另外的CAs发行客户端证书，则您需要完成以下步骤。

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。在CA证书文件的字段，请输入认证的位置，然后点击**提交**。

3. 单击 **Edit Certificate Trust List**。检查ACS应该委托的所有CAs，并且不选定ACS不应该委托的所有CAs。单击 **submit**。

重新启动服务并在 ACS 上配置 PEAP 设置

按照以下步骤重新启动服务和配置 PEAP 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 PEAP 设置，请单击 **System Configuration**，然后单击 Global Authentication Setup。
4. 选中如下所示的两个设置，并将所有其他设置保留为默认值。如果您愿意，您可以指定其他设置，例如，Enable Fast Reconnect。请在完成后单击 **Submit**。**Allow EAP-MSCHAPv2Allow MS-CHAP Version 2 AuthenticationNote:** 有关快速连接的详细信息，请参阅系统配置：身份验证和证书中的“身份验证配置选项”。