配置Cisco VPN 3000集中器4.7.x获得数字证书和SSL证书

目录

简介

本文档包括有关如何配置Cisco VPN 3000系列集中器以使用数字或身份证书和SSL证书进行身份验证的分步说明。

注意：在VPN集中器中，必须先禁用负载均衡，然后才能生成其他SSL证书，因为这会阻止证书生成。

请参阅如何使用 ASA 上的 ASDM 从 Microsoft Windows CA 获得数字证书，以便了解有关 PIX/ASA 7.x 中的相同方案的详细信息。

要了解有关Cisco IOS®平台的相同方案的详细信息，请参阅使用增强型注册命令的Cisco IOS证书注册配置示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于运行版本4.7的Cisco VPN 3000集中器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

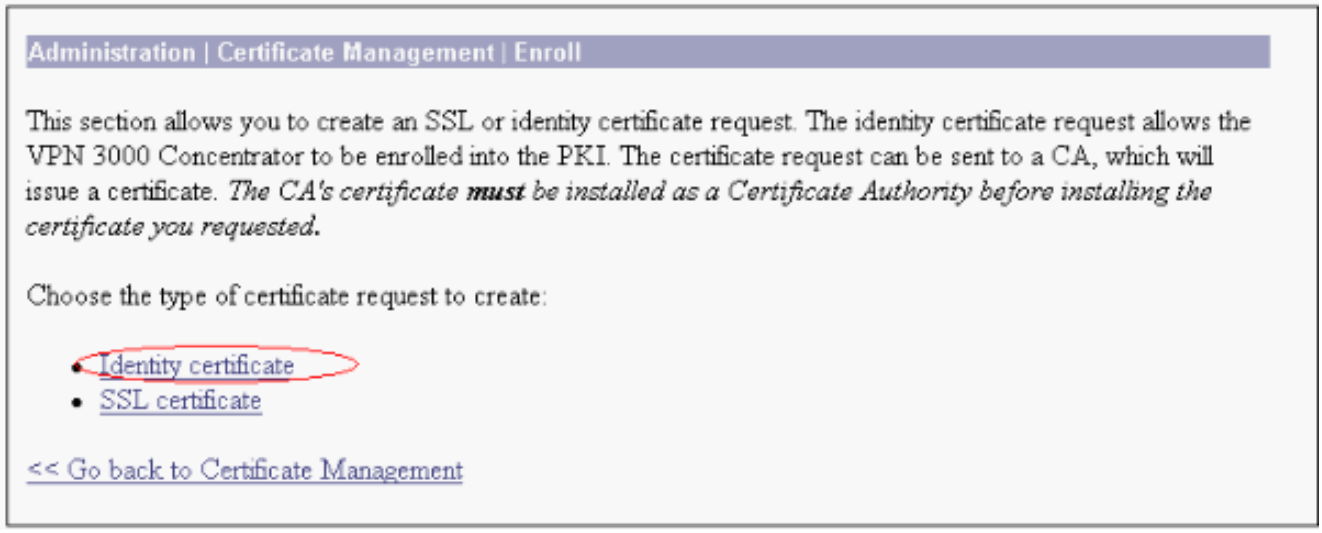
规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

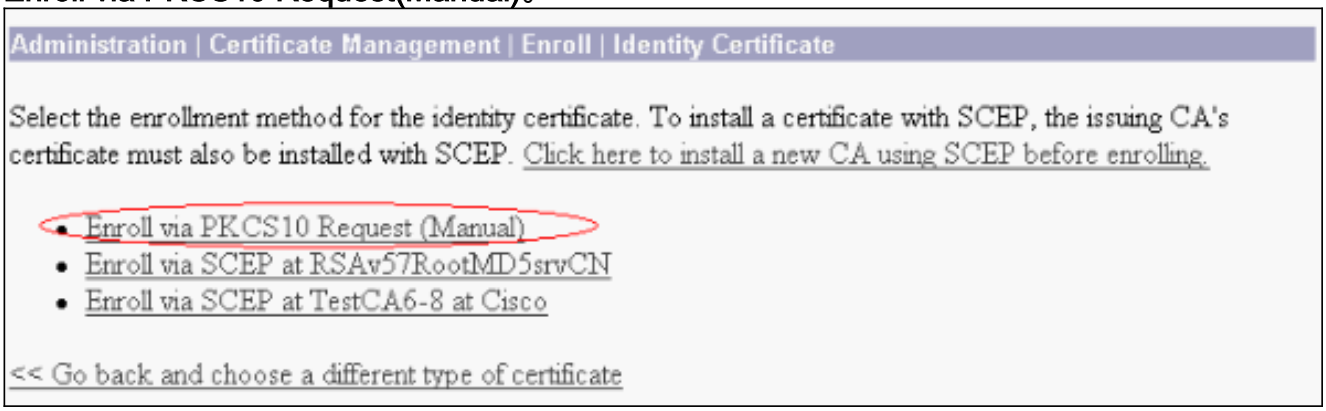
在VPN集中器上安装数字证书

请完成以下步骤：

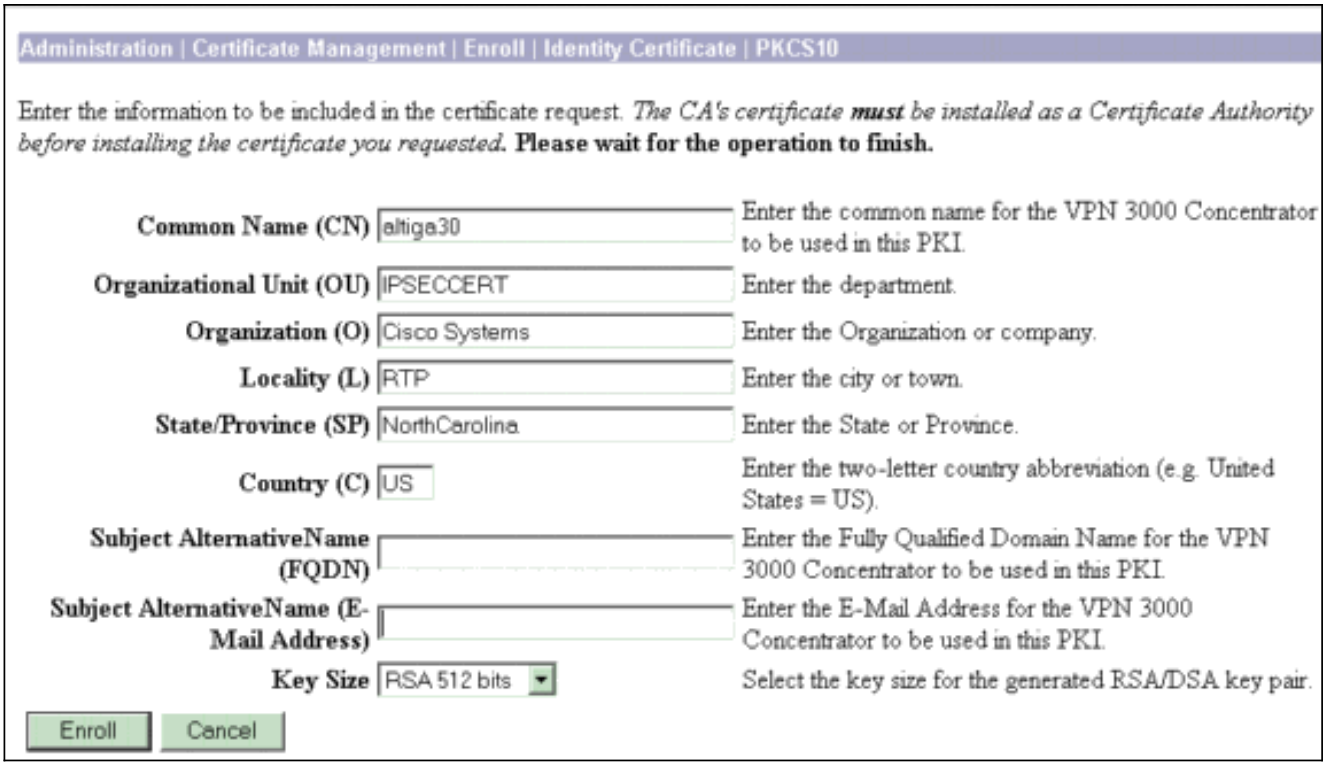
1. 选择**管理>证书管理>注**册以选择数字或身份证书请求。



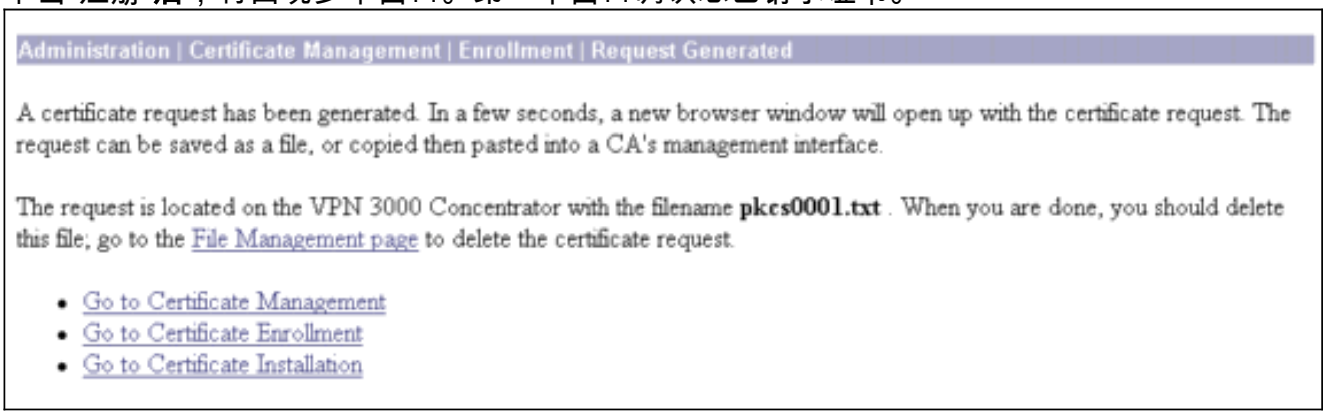
2. 选择Administration > Certificate Management > Enrollment > Identity Certificate，然后单击Enroll via PKCS10 Request(Manual)。



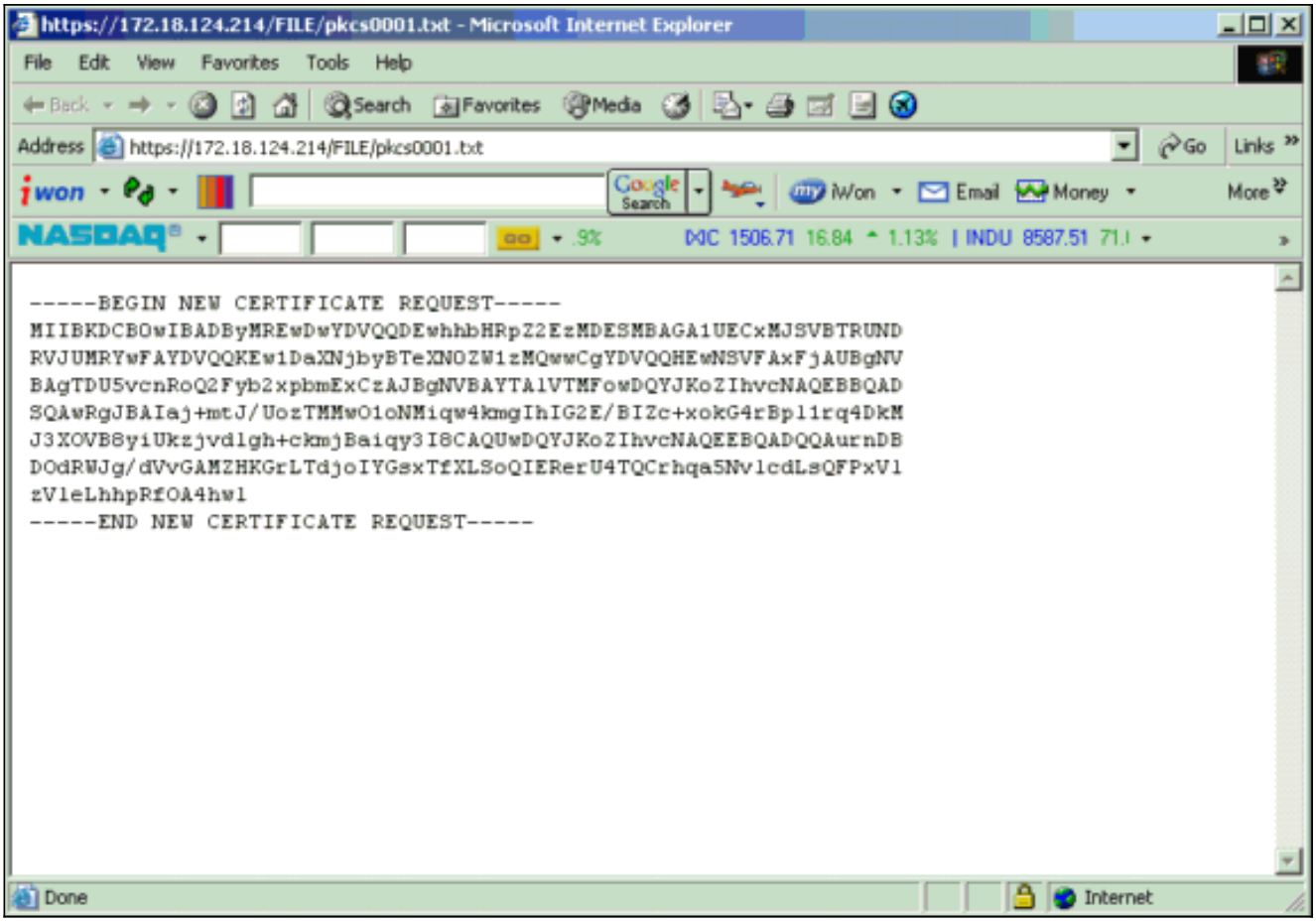
3. 填写请求的字段，然后单击“**Enroll**”。本例中填写了这些字段。**公用名**— altiga30**组织单**位 — IPSECCERT（OU应与已配置的IPsec组名匹配）**组织**- Cisco Systems**位置**— RTP**州/省** — 北卡罗来纳**国家** — 美国**完全限定域名** —（此处未使用）**密钥大**小 — 512**注：如**果使用简单证书注册协议(SCEP)请求SSL证书或身份证书，则这些是唯一可用的RSA选项。RSA 512位RSA 768位RSA 1024位RSA 2048位DSA 512位DSA 768位DSA 1024位



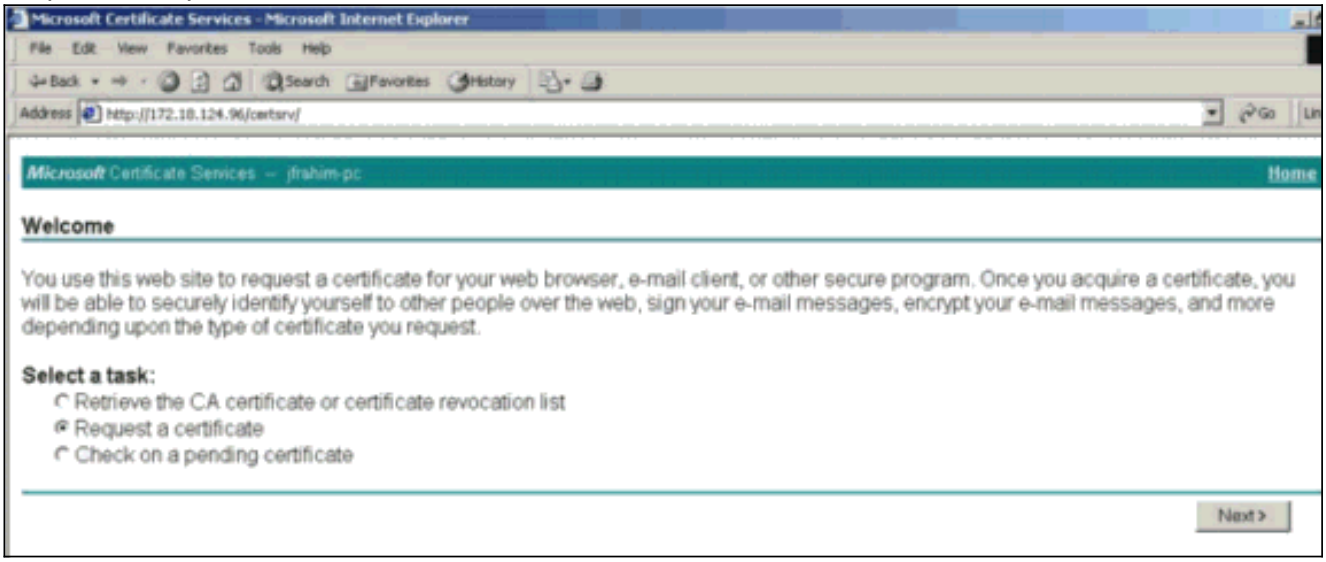
4. 单击“注册”**后**，将出现多个窗口。第一个窗口确认您已请求证书。



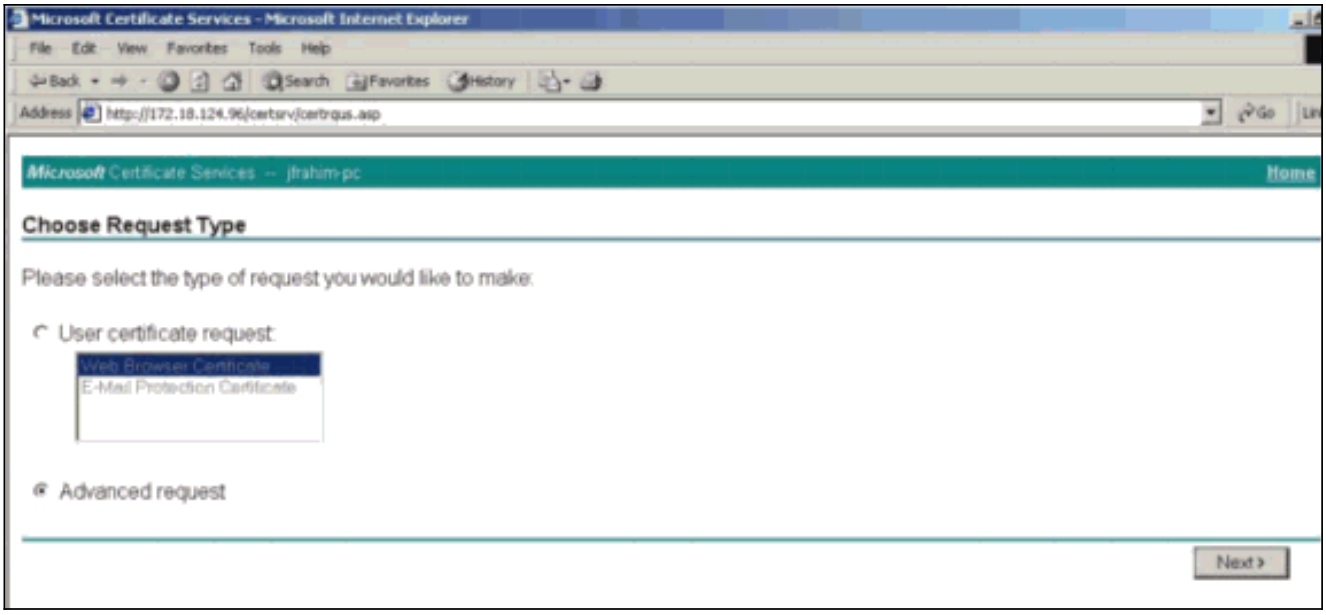
系统还会打开一个新的浏览器窗口并显示您的PKCS请求文件。



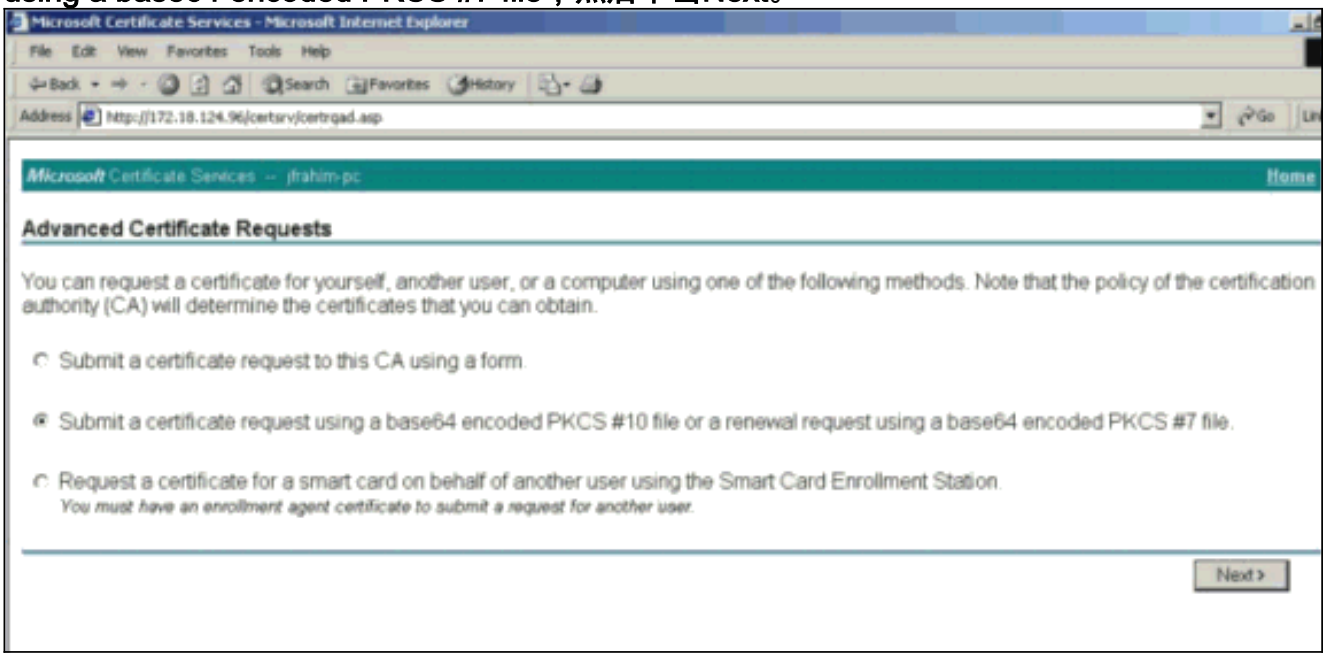
5. 在您的证书颁发机构(CA)服务器上，突出显示该请求并将其粘贴到您的CA服务器中以提交您的请求。单击 **Next**。



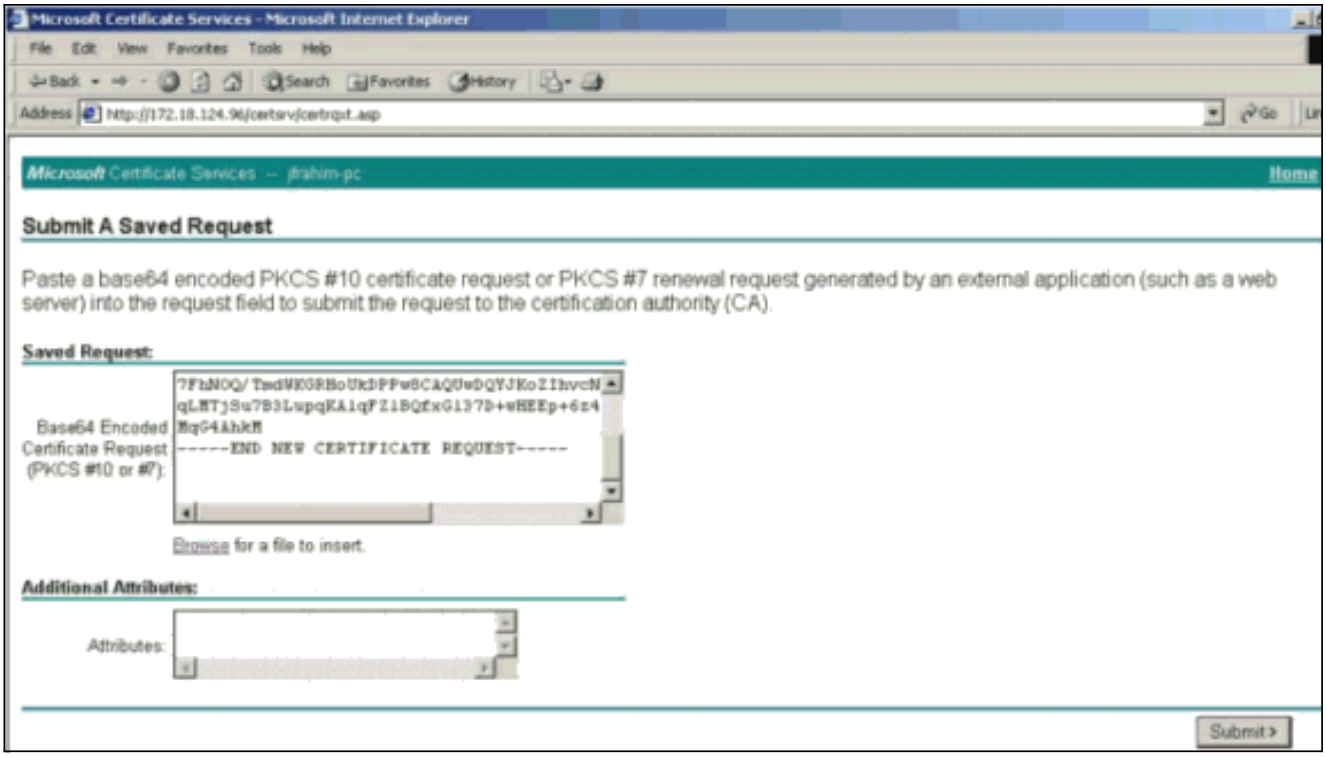
6. 选择“高**级请求”**，然后单**击“下一步”**。



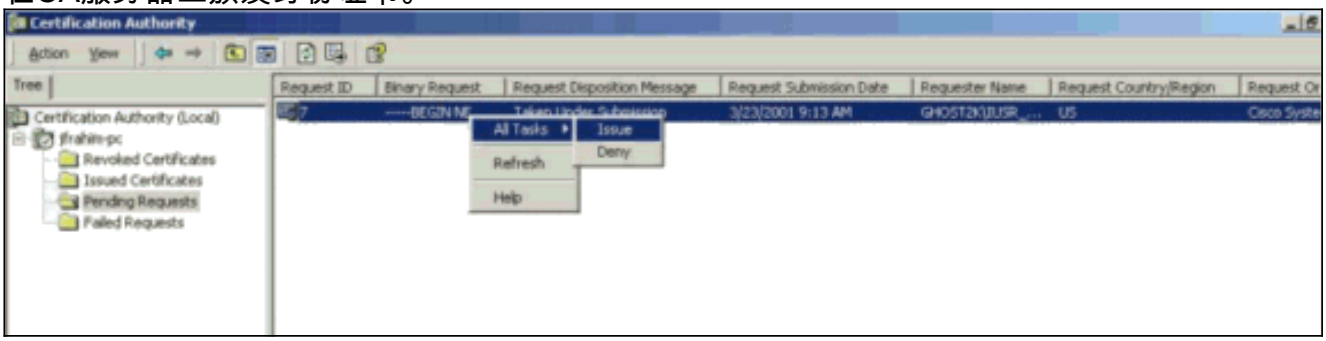
7. 选择**Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file，然后单击Next。**



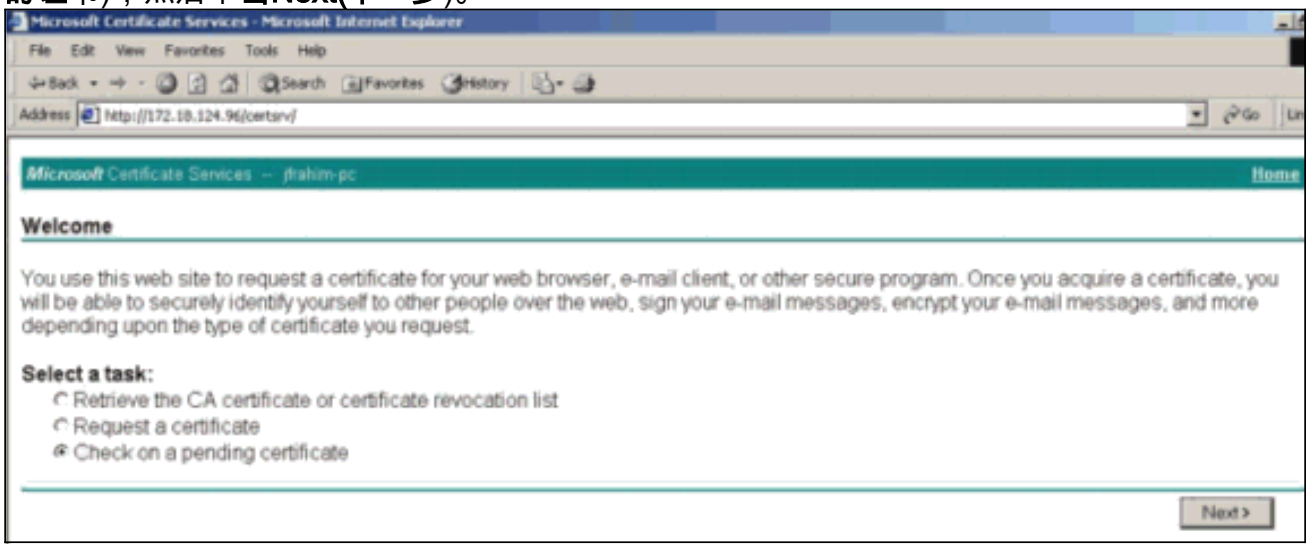
8. 将PKCS文件剪切并粘贴到Saved Request部分下的文本字段中。然后请点击**提交**。



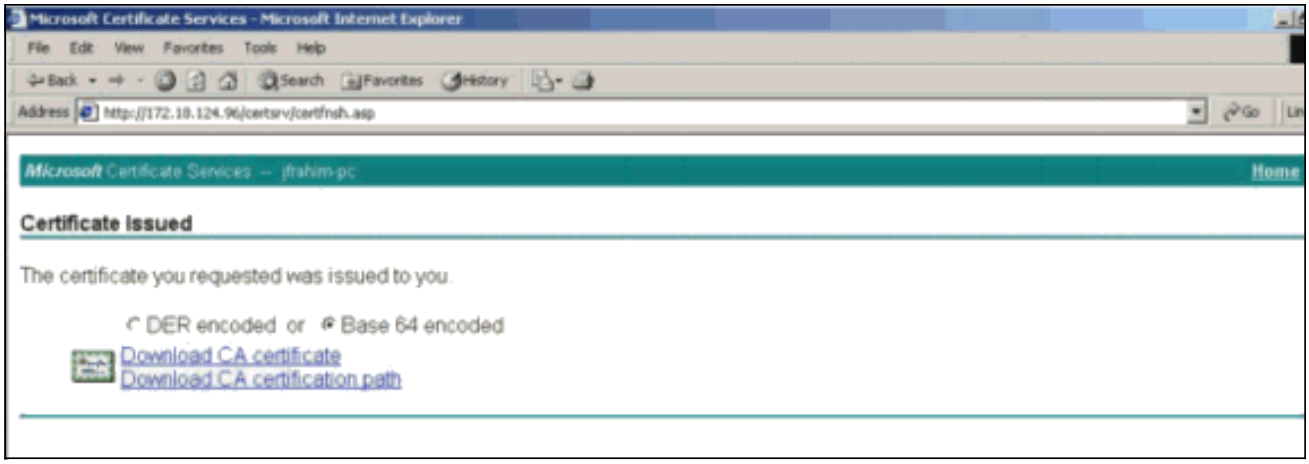
9. 在CA服务器上颁发身份证书。



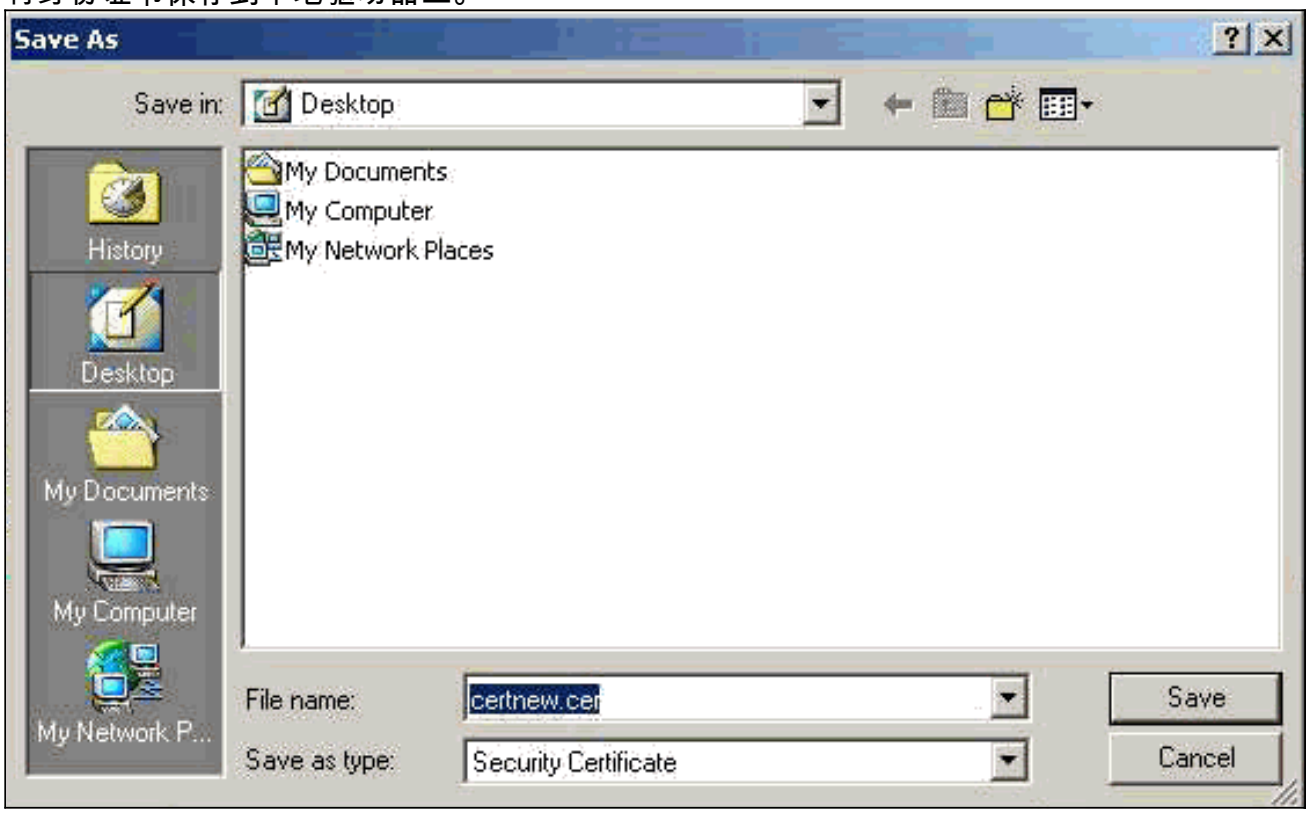
10. 下载根证书和身份证书。在您的CA服务器上，选择**Check on a pending certificate(检查挂起的证**书)，然后单**击Next(下一步**)。



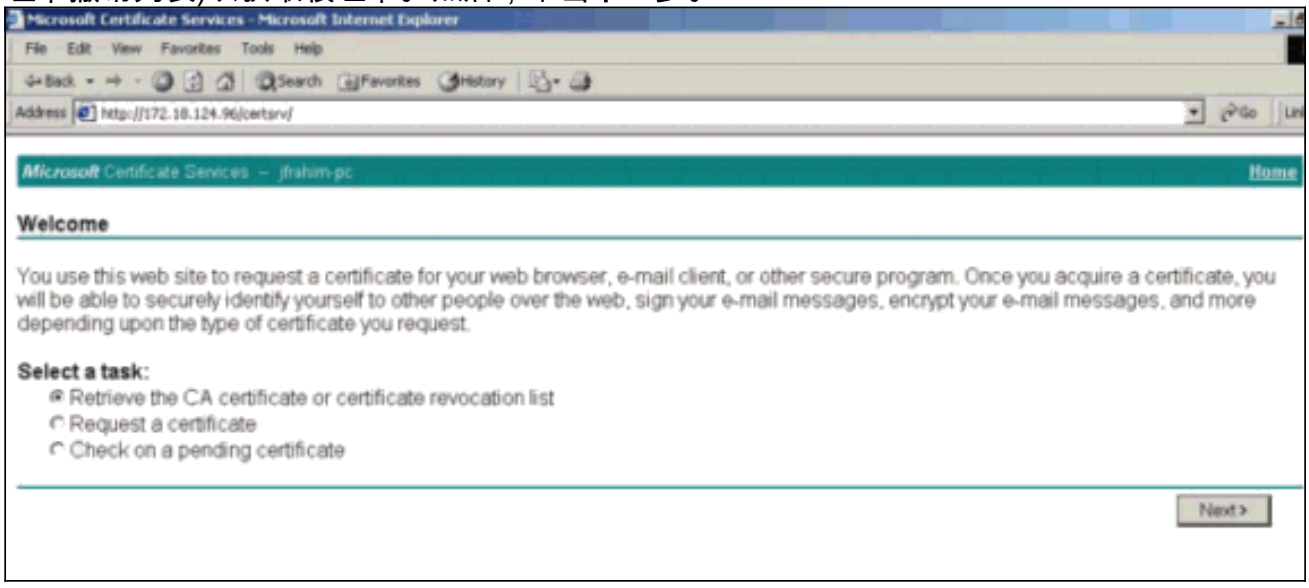
11. 选择**Base 64 encoded**，然后单击**Download CA certificate on** the CA server。



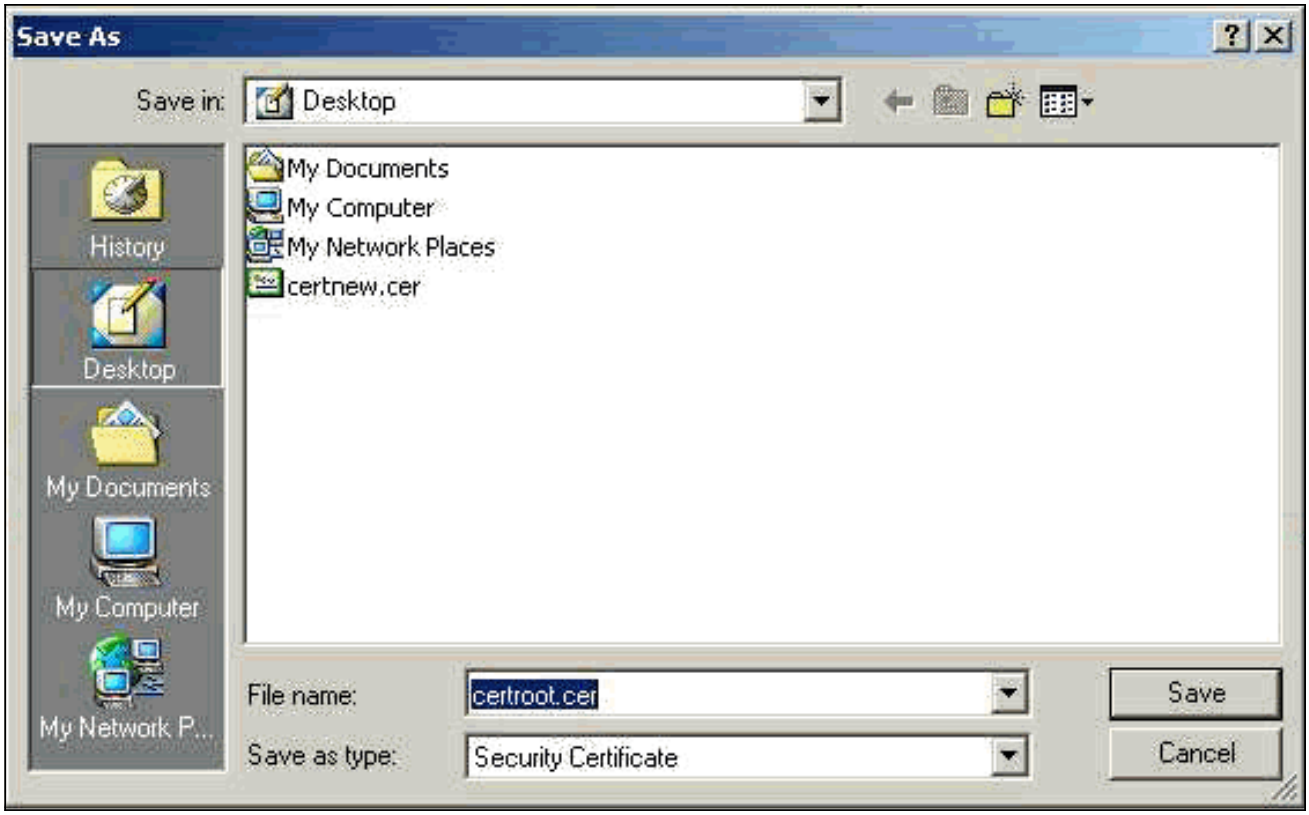
12. 将身份证书保存到本地驱动器上。



13. 在CA服务器上，选择**Retrieve the CA certificate or certificate revocation list(检索CA证书或证书撤销列表)**以获取根证书。然后，单击**下一步**。



14. 将根证书保存到本地驱动器上。



15. 在VPN 3000集中器上安装根证书和身份证书。为此，请选择**Administration > Certificate Manager > Installation > Install certificate avaried via enrollment**。在“Enrollment Status”下，单击**Install**。

Administration | Certificate Management | Install certificate obtained via enrollment

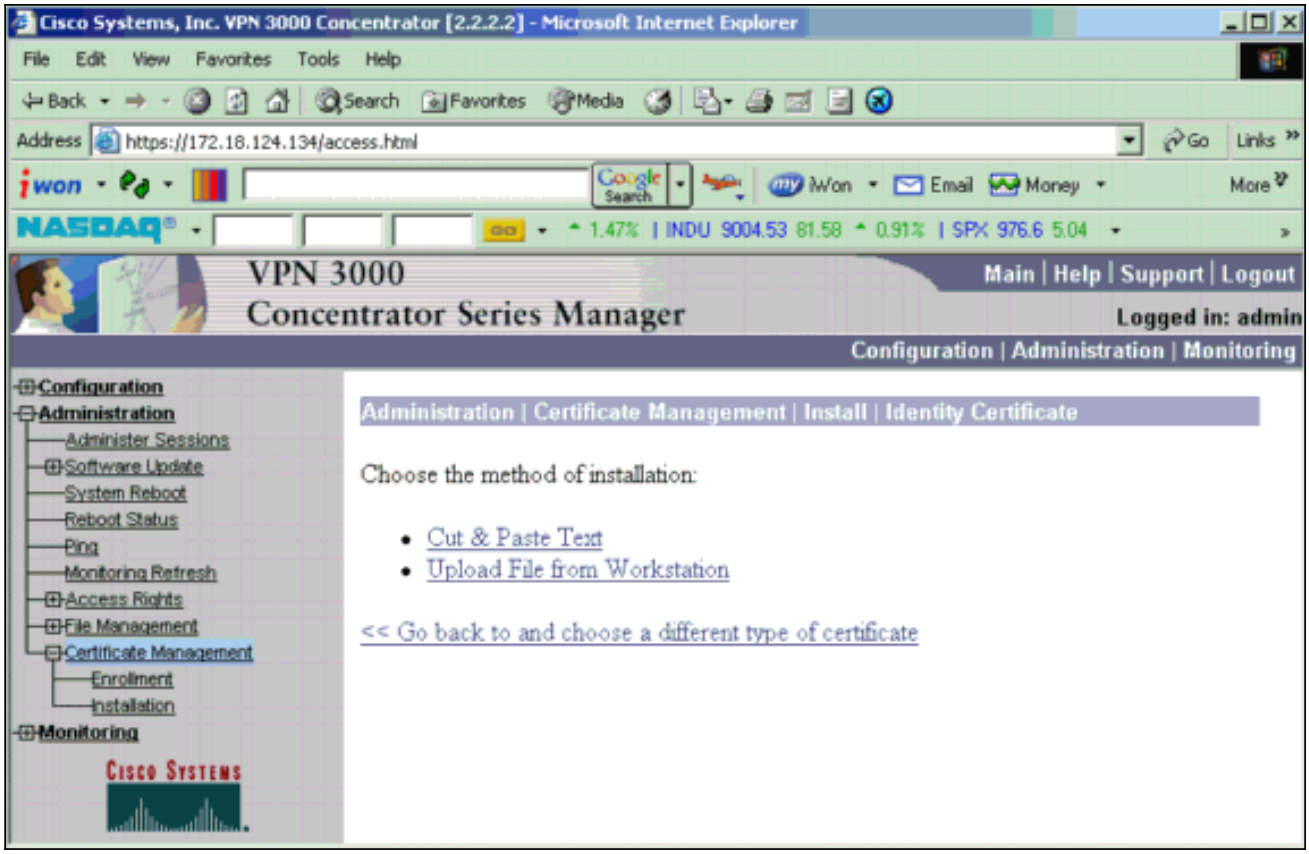
Select a enrollment request to install.

Enrollment Status

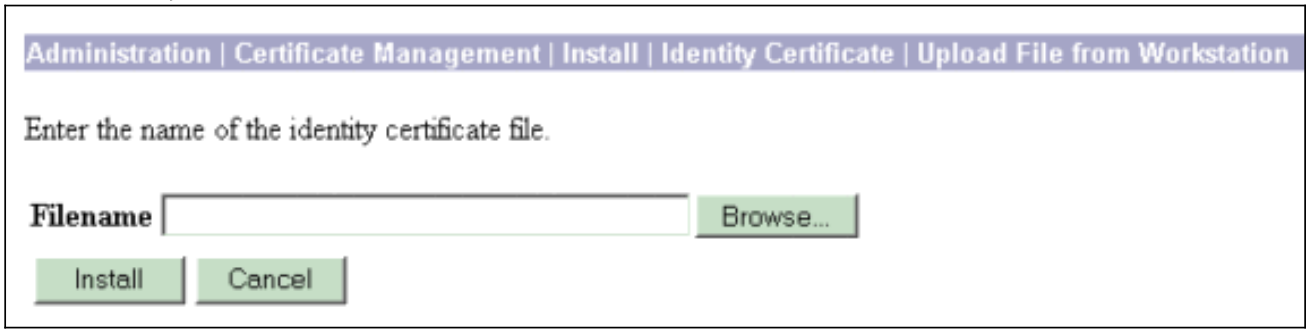
Subject	Issuer	Date	Use	Reason	Method	Status	Actions
altiga30 at Cisco Systems	*N/A*	05/22/2003	ID	Initial	Manual	In Progress	View | Install | Delete

<< Go back and choose a different type of certificate

16. 单击“**从工作站上传文件**”。



17. 单击**Browse**并选择您保存到本地驱动器的根证书文件。选择**Install**以在VPN集中器上安装身份证书。管理 | Certificate Management窗口显示为确认，您的新身份证书显示在Identity Certificates表中。



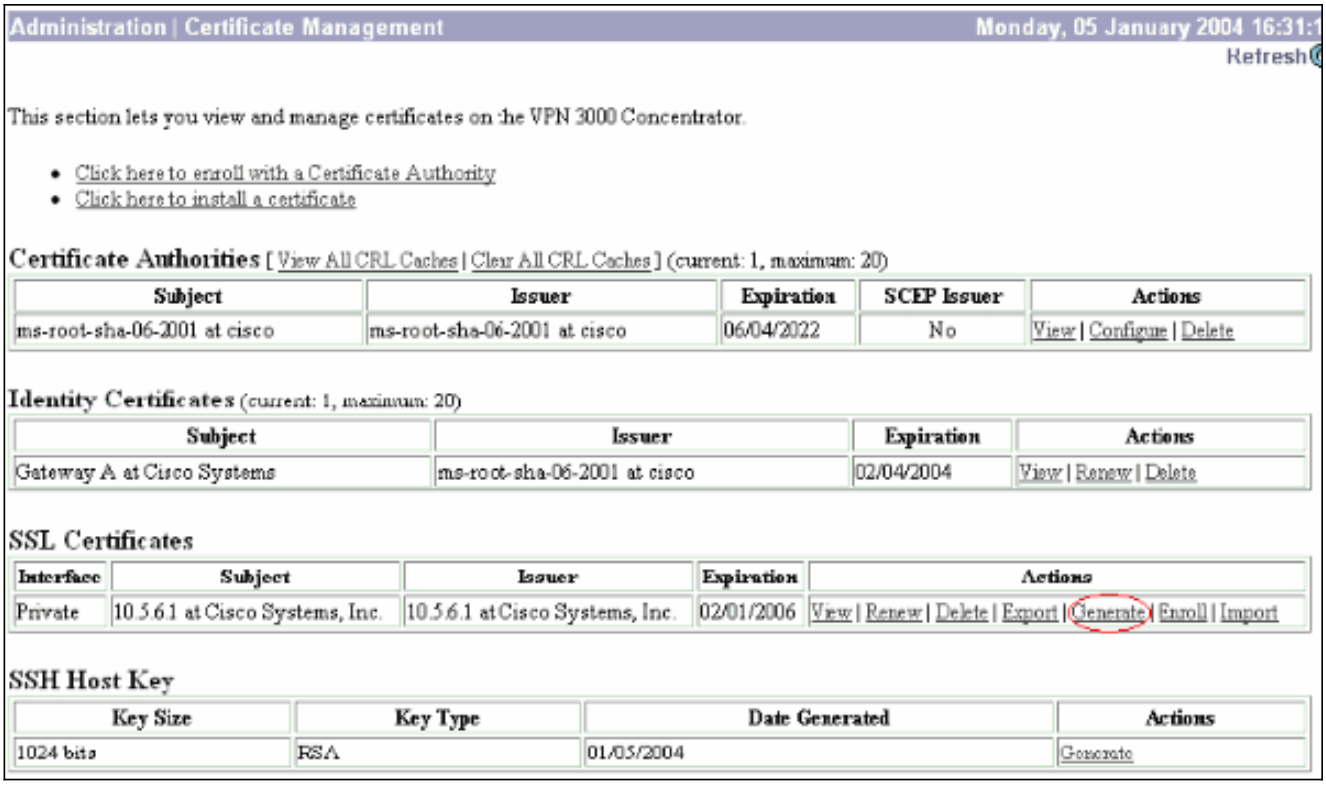
注意：如果证书失败，请完成以下步骤以生成新证书。选择 **Administration > Certificate Management**。在SSL证书列表的“操作”(Actions)框中单击**删除**。选择**管理>系统重新启动**。选**择Save the active configuration at time of reboot，选择Now**，然**后单**击**Apply**。重新加载完成后，您现在可以生成新证书。

在VPN集中器上安装SSL证书

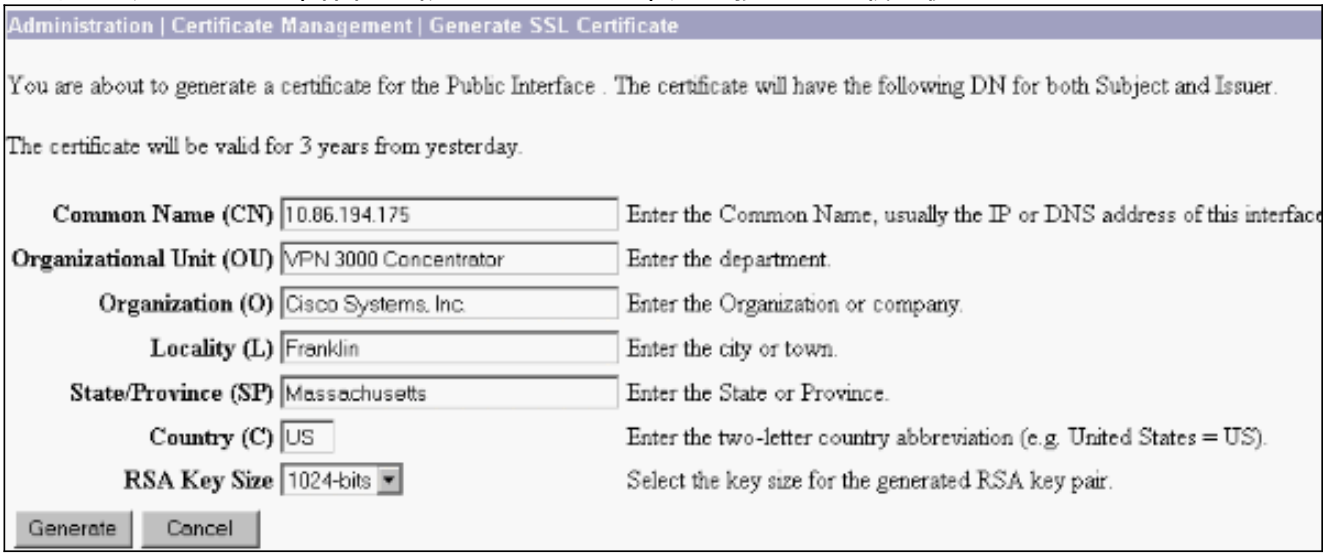
如果在浏览器和VPN集中器之间使用安全连接，则VPN集中器需要SSL证书。您还需要在用于管理VPN集中器和WebVPN的接口上以及用于终止WebVPN隧道的每个接口上的SSL证书。

升级VPN 3000集中器软件后，当VPN 3000集中器重新启动时，接口SSL证书（如果不存在）将自动生成。由于自签名证书是自生成的，因此此证书不可验证。没有证书颁发机构保证其身份。但是，此证书允许您使用浏览器与VPN集中器进行初始联系。如果要将其替换为另一个自签名SSL证书，请完成以下步骤：

1. 选择**管理>证书管理**。



2. 单击**Generate**以在SSL Certificate表中显示新证书并替换现有证书。此窗口允许您为VPN集中器自动生成的SSL证书配置字段。这些SSL证书用于接口和负载均衡。



如果要获取可验证的SSL证书（即由证书颁发机构颁发的证书），请参阅本文档的在VPN集中器上安装数字证书部分，以便使用用于获取身份证书的相同过程。但是，此时，在Administration > Certificate Management **> Enroll窗口**中，单击**SSL证**书（而不是Identity Certificate）。**注意：**请参阅管*理 | VPN 3000集中*器参考卷II的证书管理部分：管理和监控版本4.7，了解有关数字证书和SSL证书的完整信息。

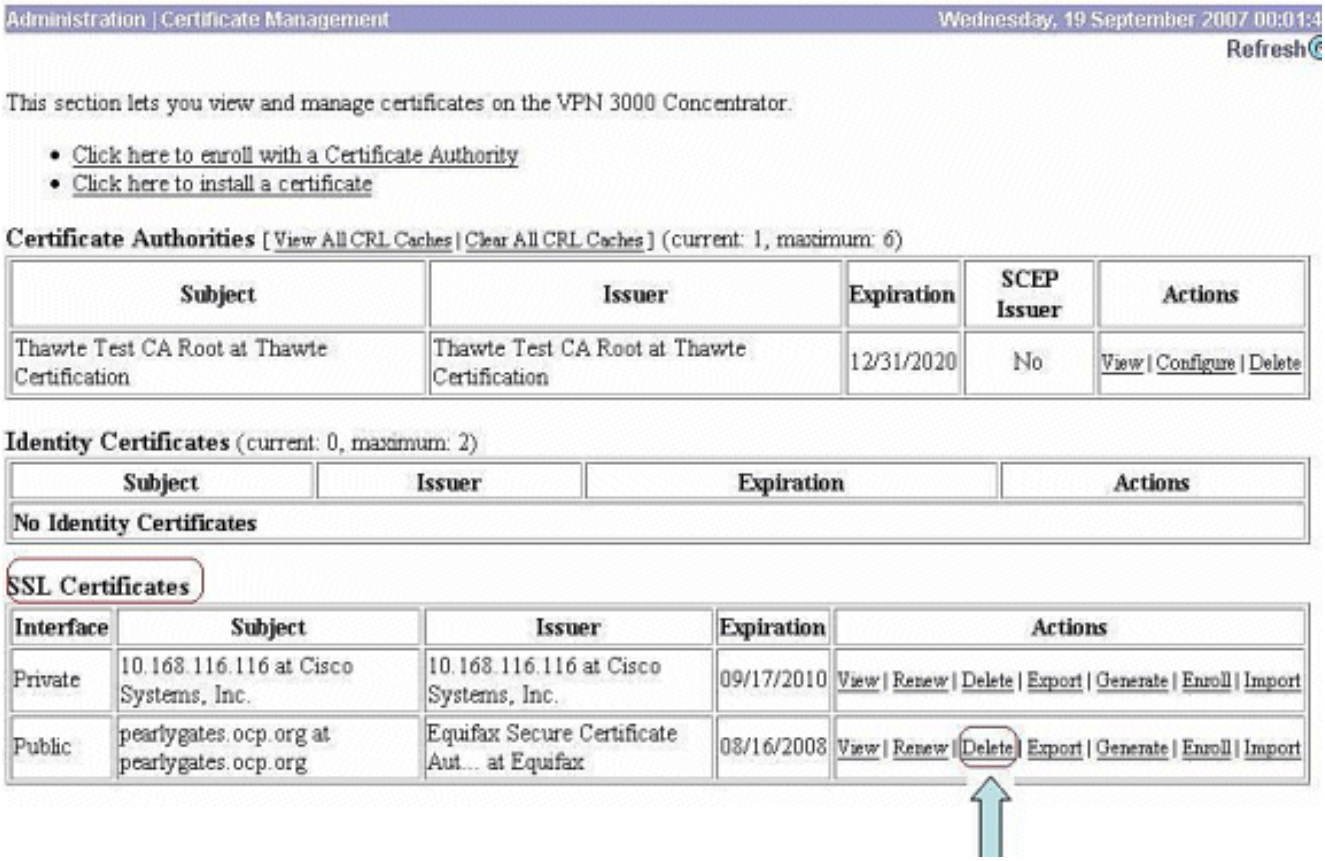
在VPN集中器上更新SSL证书

本节介绍如何续约SSL证书：

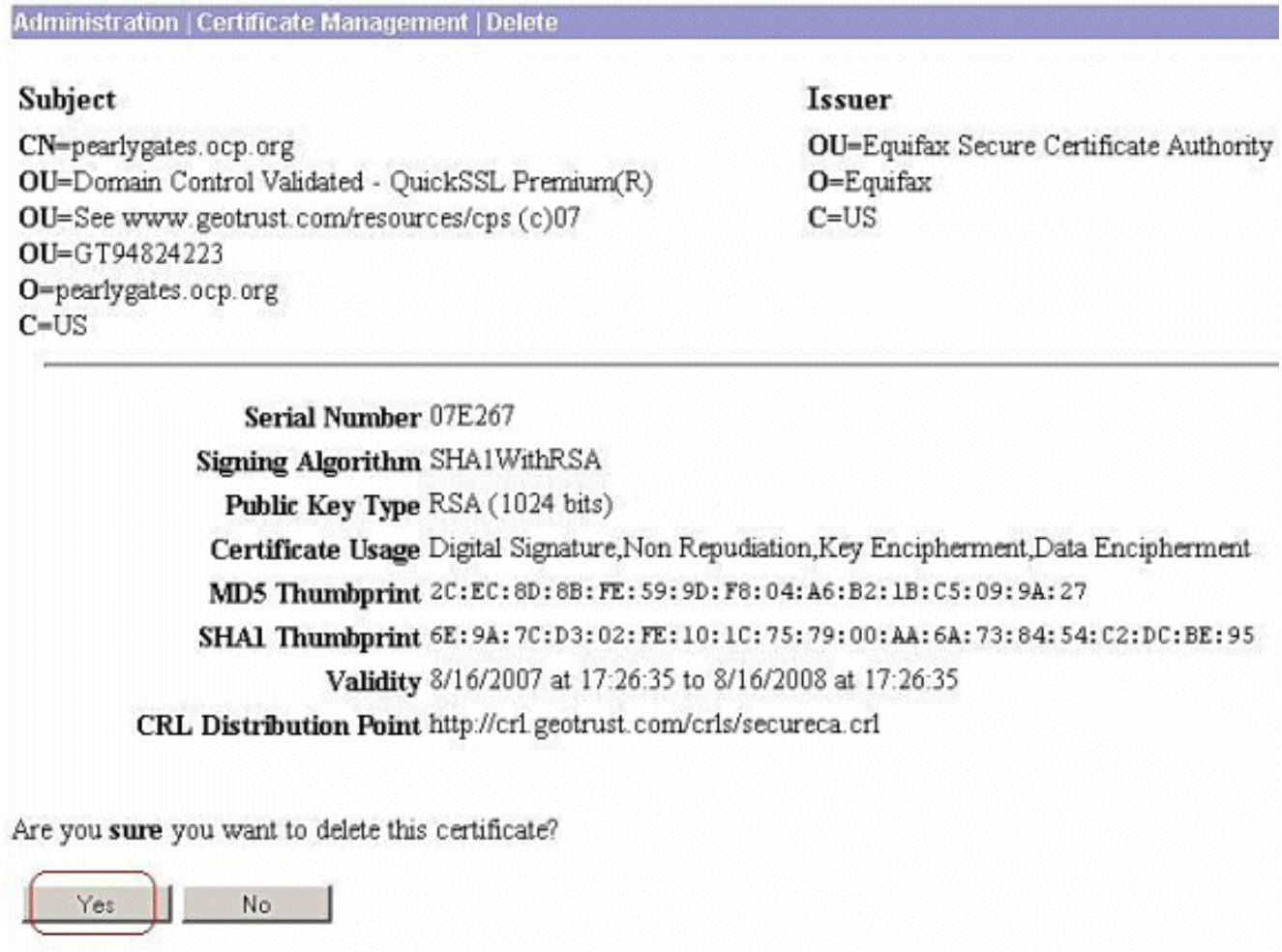
如果这是VPN集中器生成的SSL证书，请转至SSL部分的**Administration > Certificate Management**。单击**renew**选项，然后该选项将更新SSL证书。

如果这是外部CA服务器授予的证书，请完成以下步骤：

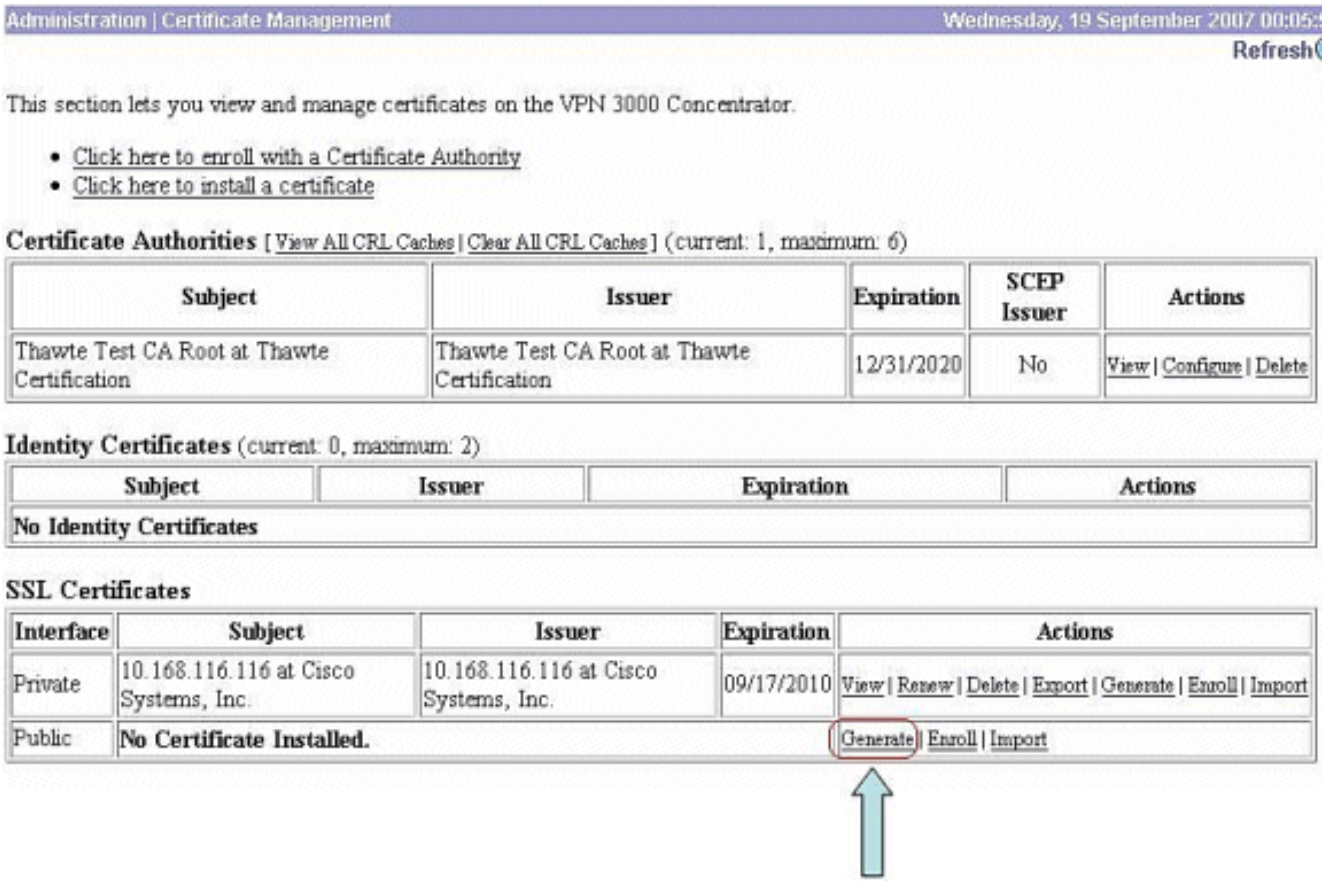
1. 在*SSL Certificates*下选择**Administration > Certificate Management >Delete，以便从公共接口删除过期的证书。**



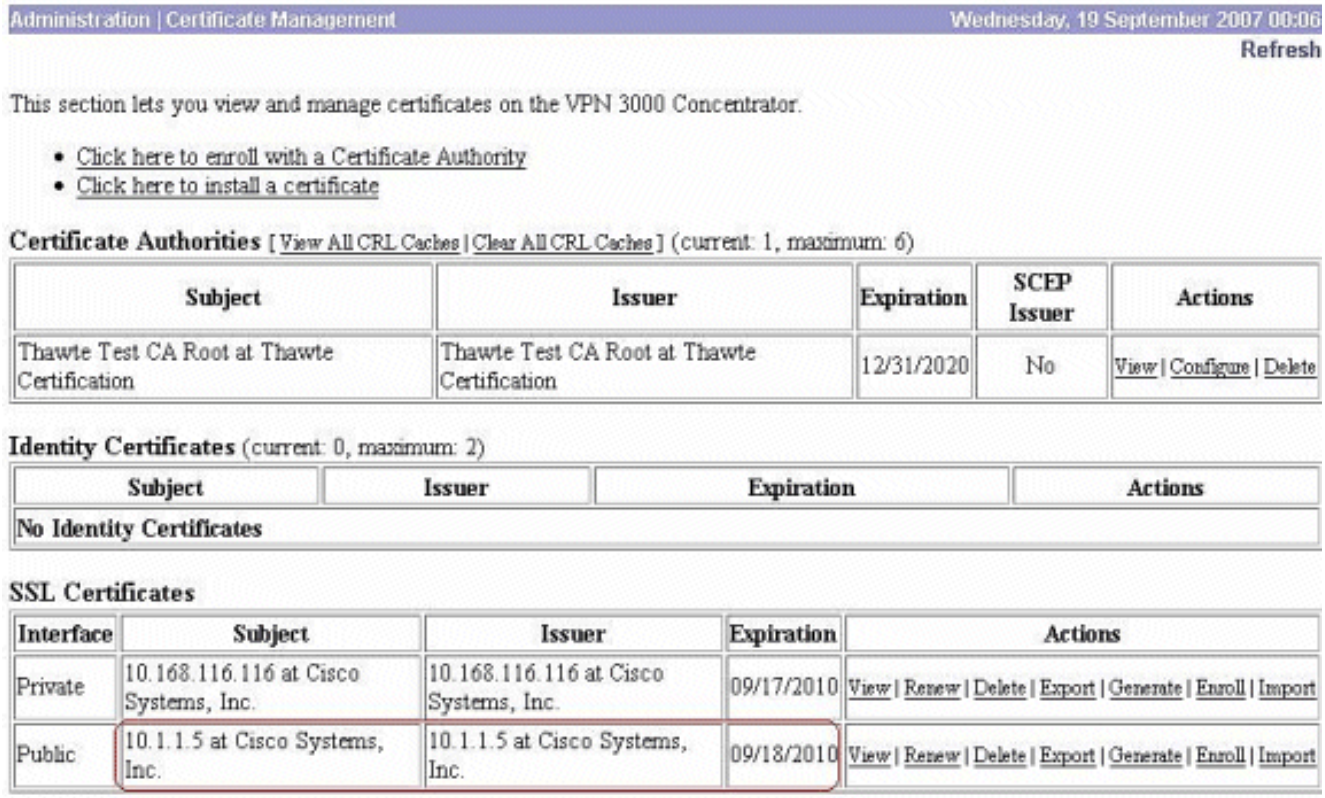
单击**Yes**以确认删除SSL证书。



2. 选择**Administration > Certificate Management > Generate**以生成新的SSL证书。



系统将显示公共接口的新SSL证书。



相关信息

- Cisco VPN 3000 系列集中器支持页
- IPsec 协商/IKE 协议
- 技术支持和文档 - Cisco Systems