ASA 8.X：AnyConnect SCEP登记配置示例

目录

简介

SCEP登记功能在AnyConnect独立客户端2.4介绍。在此进程，您修改AnyConnect XML配置文件包括一SCEP相关配置和创建一个特定组策略和连接配置文件证书登记的。当AnyConnect用户连接给此特定组时， AnyConnect发送证书登记请求到CA服务器，并且CA服务器自动地接受或拒绝请求。

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以下软件和硬件版本：

- 运行软件版本 8.x 的 Cisco ASA 5500 系列自适应安全设备
- Cisco AnyConnect VPN版本2.4

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

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

自动SCEP登记目标AnyConnect的是发行证书对客户端以安全和可扩展方式。例如，用户不需要请求从CA服务器的一证书。此功能在AnyConnect客户端集成。证书发出给根据证书参数的客户端提及在XML配置文件。

要求的更改概述

AnyConnect SCEP登记功能要求在XML配置文件将定义的某些证书参数。组策略和连接配置文件在证书登记的ASA创建，并且XML配置文件关联与该策略。AnyConnect客户端连接对使用此特定策略的连接配置文件并且发送一个要求与在XML文件定义的参数的一证书。Certificate Authority (CA)自动地接受或拒绝请求。如果<CertificateSCEP>元素在客户端配置文件，定义AnyConnect客户端获取与SCEP协议的证书。

客户端证书验证必须发生故障，在AnyConnect设法自动地获取新的证书前，因此，如果已经安排一个有效证书安装，登记不发生。

当对特定组的用户登录，他们自动地登记。也有用户用**获得证书**按钮提交的证书检索的一手工方法联机。这只运作，当客户端有直接访问到CA服务器，不通过通道。

参考Cisco AnyConnect VPN客户管理员指南，版本2.4欲知更多信息。

启用Anyconnect SCEP功能的XML设置

这些是在AnyConnect XML文件需要定义的要素。参考Cisco AnyConnect VPN客户管理员指南，版本2.4欲知更多信息。

- <AutomaticSCEPHost> —指定ASA主机名和连接配置文件(隧道组) SCEP证书检索配置。值需要在ASA \连接配置文件名称的ASA \连接配置文件名称或者IP地址的完全限定域名的格式。
- <CAURL> —识别SCEP CA服务器。
- <CertificateSCEP> —定义了证书的内容如何是请求的。
- <DisplayGetCertButton> —确定AnyConnect GUI是否显示获得证书按钮。它使用户手工请求证书的续订或供应。

这是示例配置文件：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false</LocalLanAccess>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
     ReconnectAfterResume
```

```
   </AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
    Automatic
  </RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Automatic
<PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="false">false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
     http://10.11.11.1/certsrv/mscep/mscep.dll
   </CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

配置ASA支持AnyConnect的SCEP协议

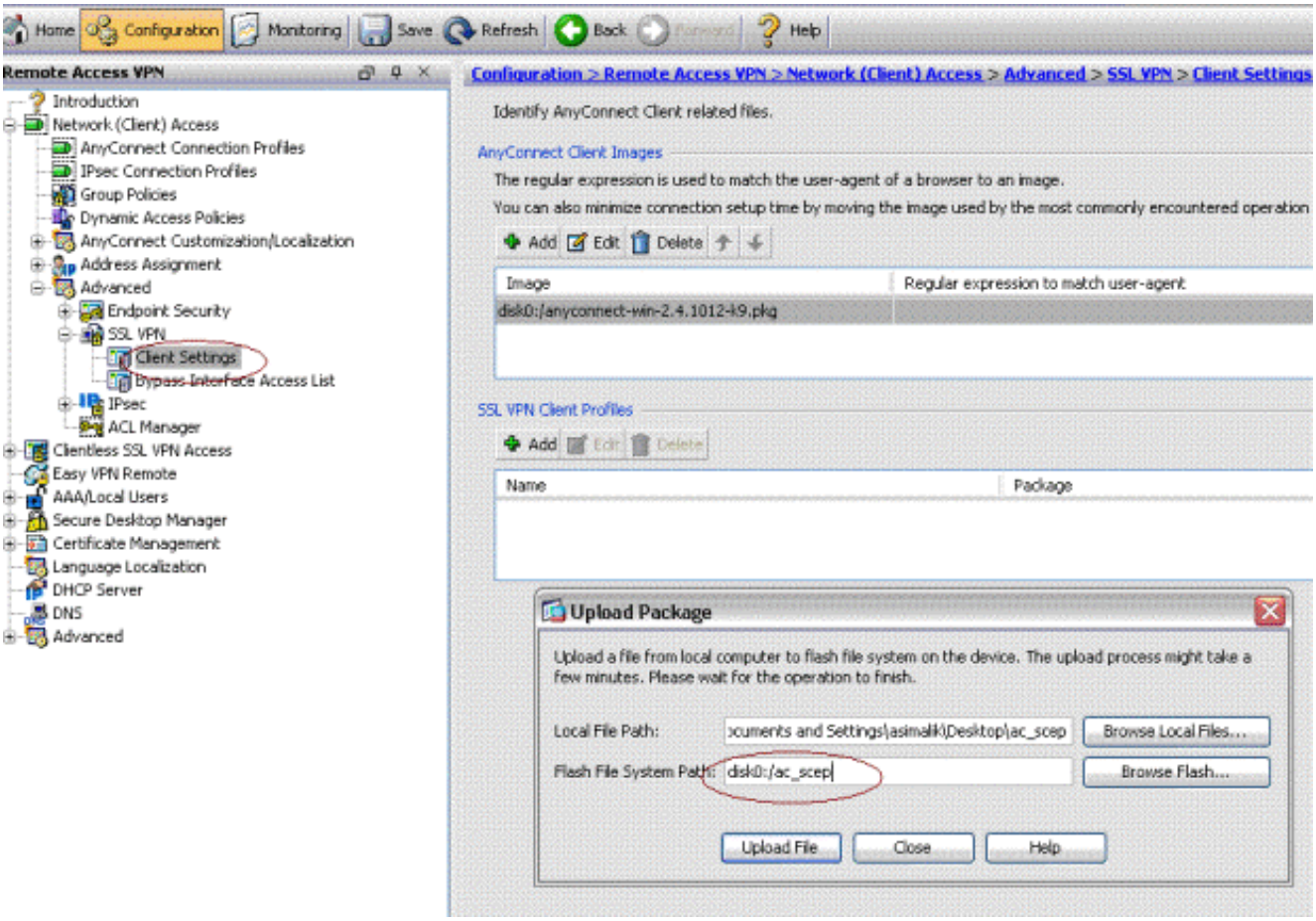
为了提供存取对于私有注册机关(RA)，有ACL限制内部侧网络连通性对希望的RA的ASA管理员必须创建别名。为了自动地获取证书，用户连接并且验证对此别名。

完成这些步骤：

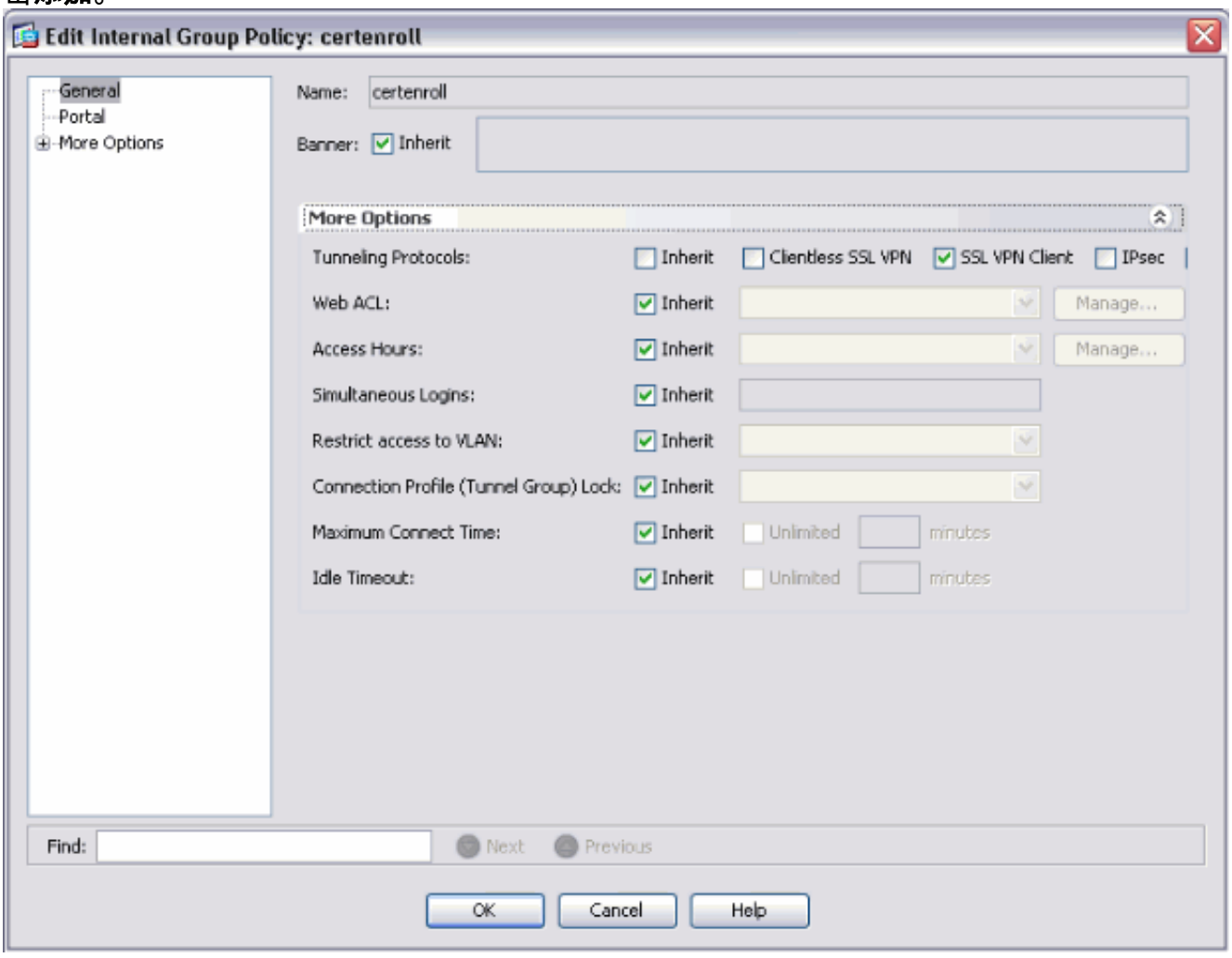
1. 创建在ASA的一别名指向特定已配置组。
2. 指定在<AutomaticSCEPHost>元素的别名在用户的客户端档案。
3. 附加包含<CertificateEnrollment>部分对特定已配置组的客户端配置文件。
4. 设置特定已配置组的ACL限制流量到内部侧RA。

完成这些步骤：

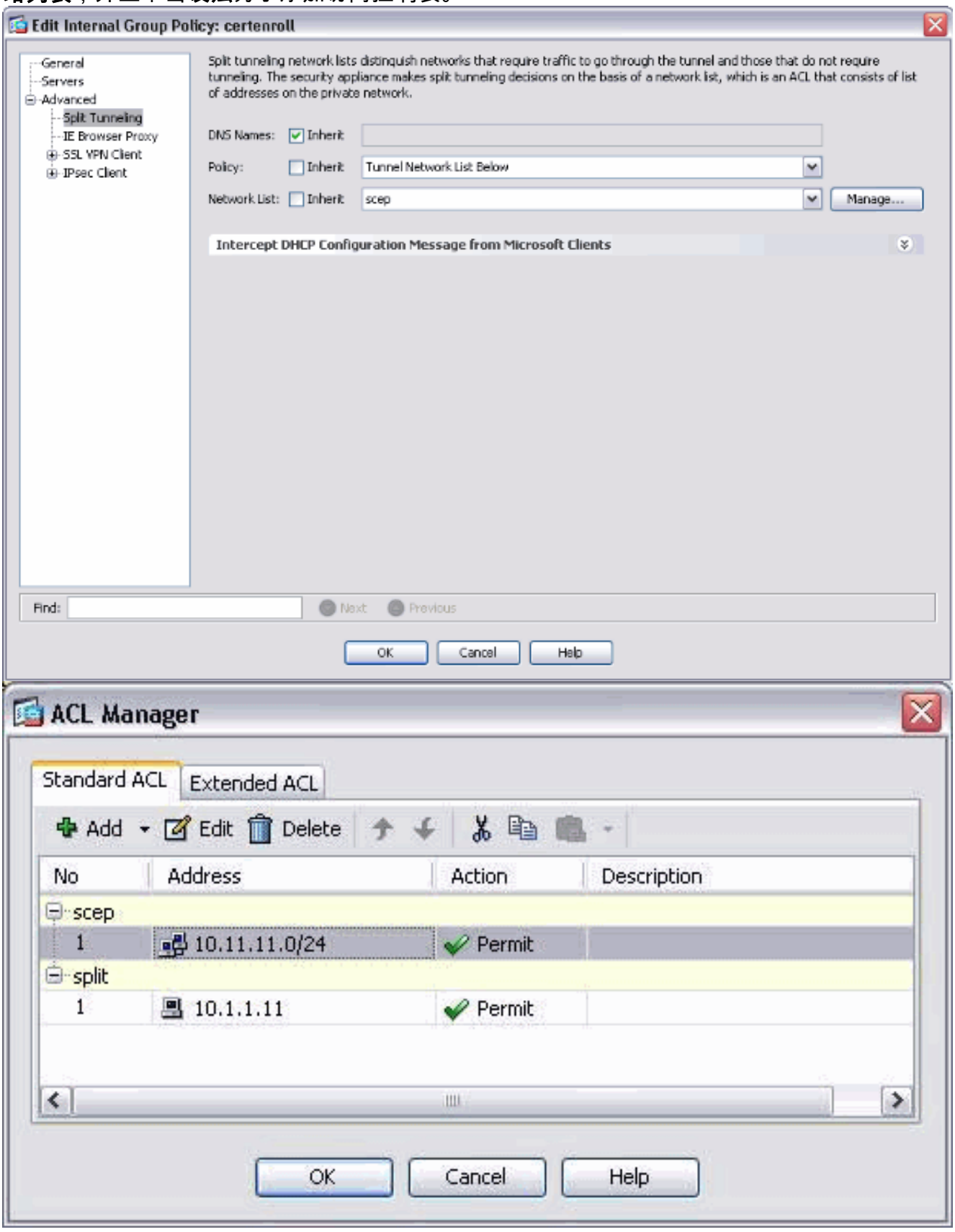
1. 上传XML配置文件对ASA。选择**远程访问VPN >网络(客户端)访问>Advanced > SSL VPN >客户端设置**。在SSL VPN客户端配置文件下，请单击**添加**。单击**浏览本地文件**为了选择配置文件，并且单击**浏览闪存**为了指定闪存文件名。单击 **Upload File**。



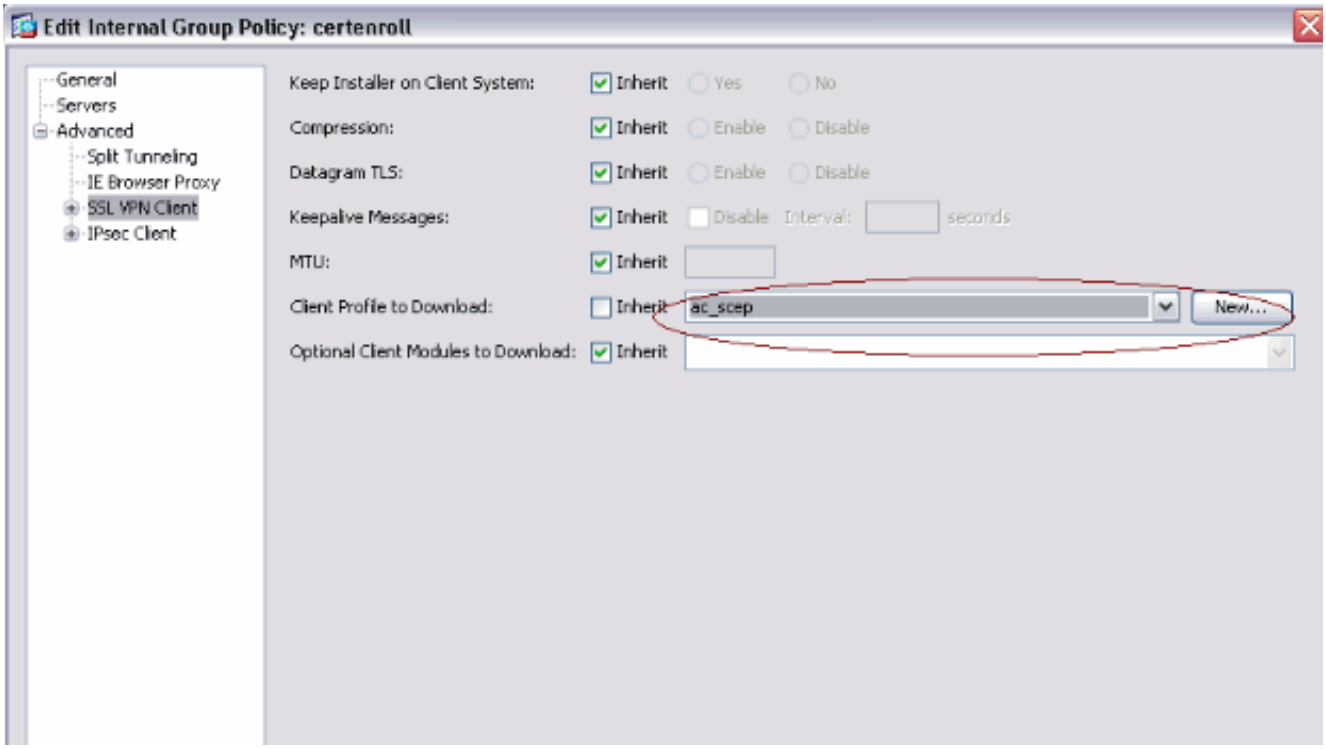
2. 设置证书登记的一项certenroll组策略。选择**远程访问VPN >网络客户端访问>组策略**，并且单击**添加**。



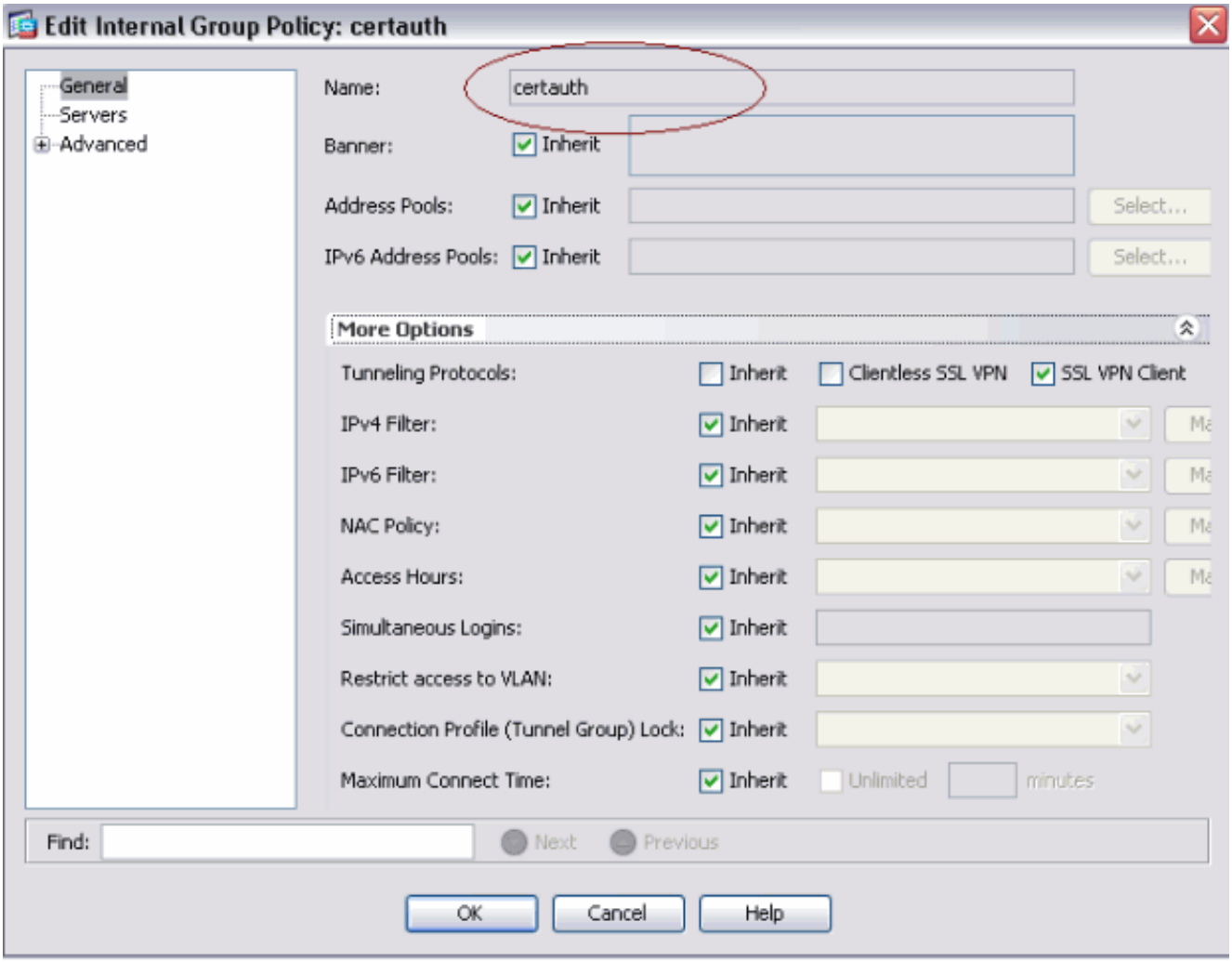
添加CA服务器的一个分割隧道。展开**先进**，然后选择**分割隧道**。从策略菜单选择**如下隧道网络列表**，并且单击**设法**为了添加访问控制表。



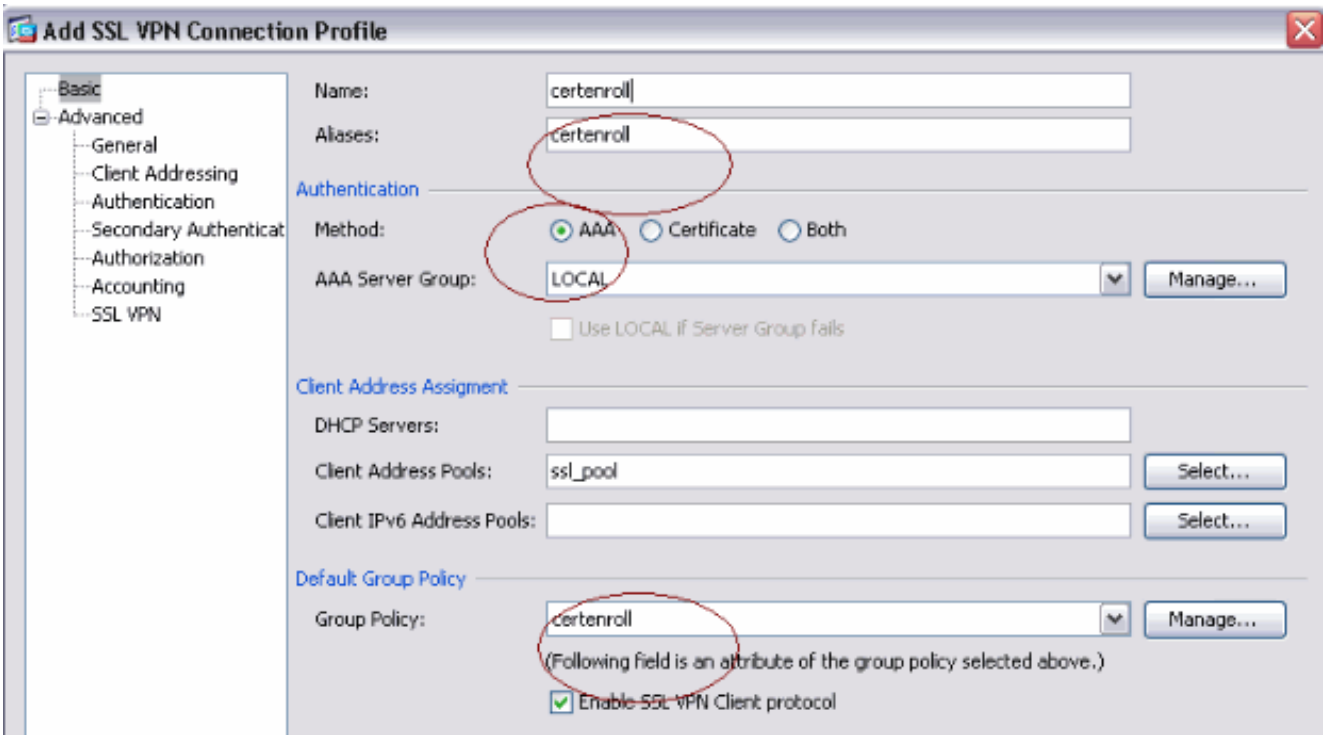
选择**SSL VPN客户端**，并且从**客户端配置文件**选择certenroll的配置文件**到Download菜单**。



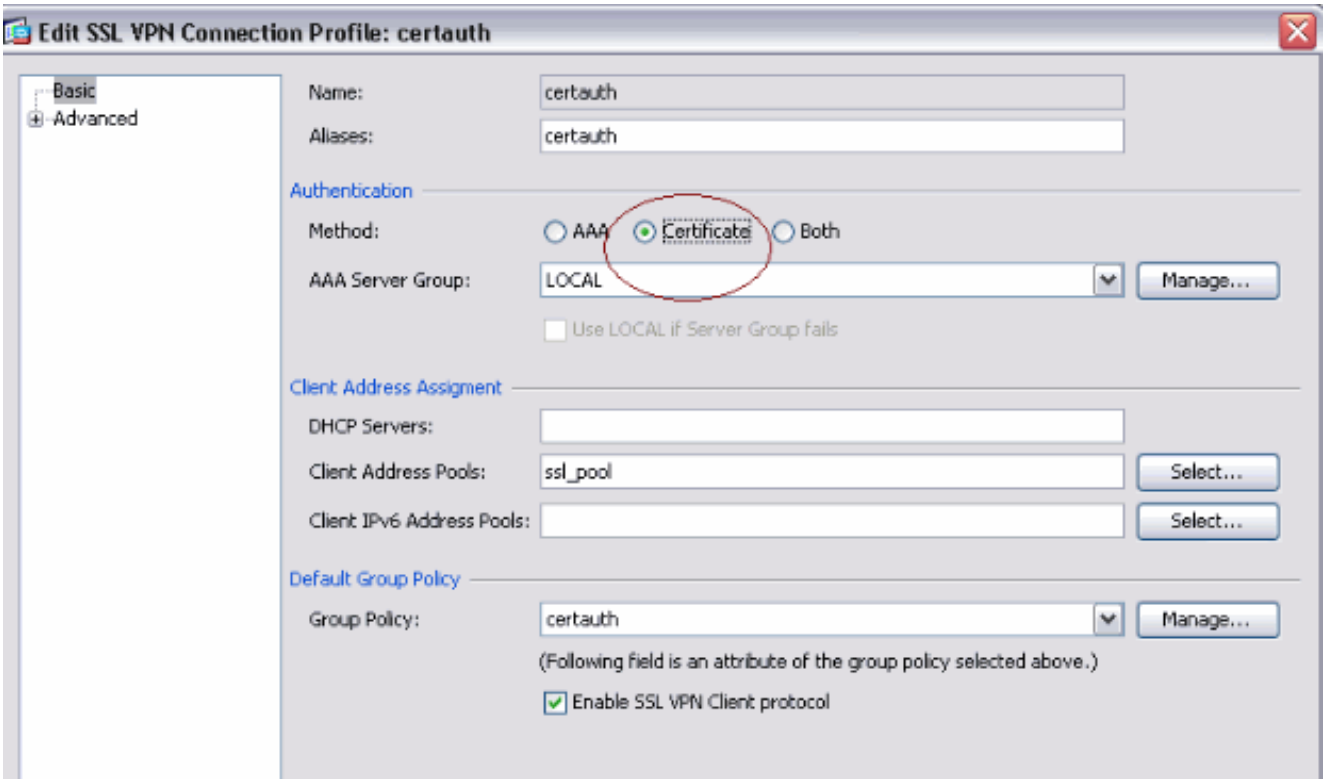
3. 创建另一组呼叫证书验证的**certauth**。



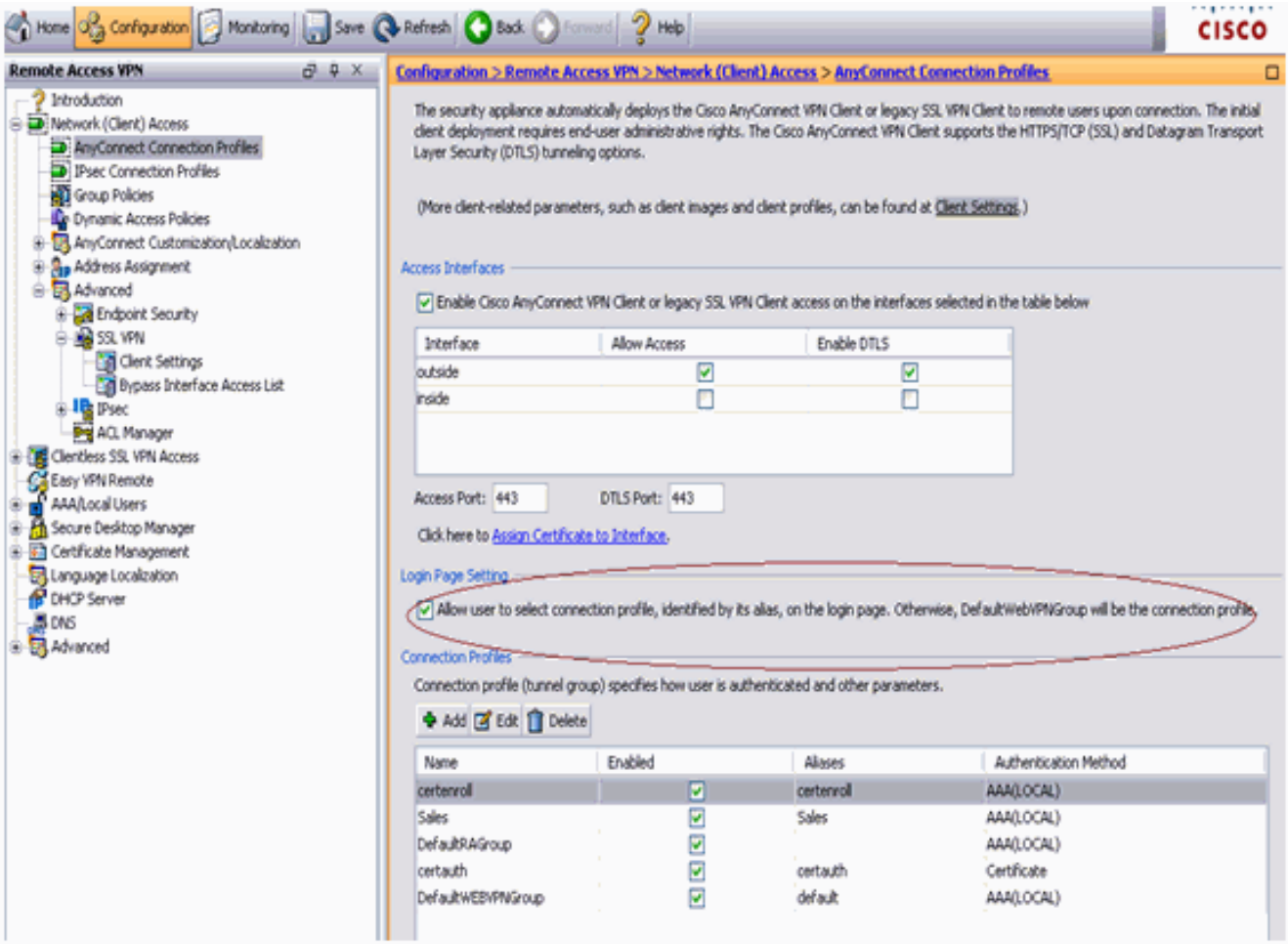
4. 创建certenroll连接配置文件。选择**远程访问VPN >网络客户端访问> AnyConnect连接配置文件**，并且单击**添加**。在别名字段输入**certenroll**组。**注意：** 别名必须匹配用于AnyConnect配置文件的值在AutomaticSCEPHost下。



5. 做呼叫与证书验证的**certauth的**另一个连接配置文件。这是在登记以后使用的实际连接配置文件。



6. 为了确保使用别名启用，检查**允许用户选择连接配置文件，识别由其别名，在登录页。否则，DefaultWebVPNGroup是连接配置文件。**



测验AnyConnect SCEP

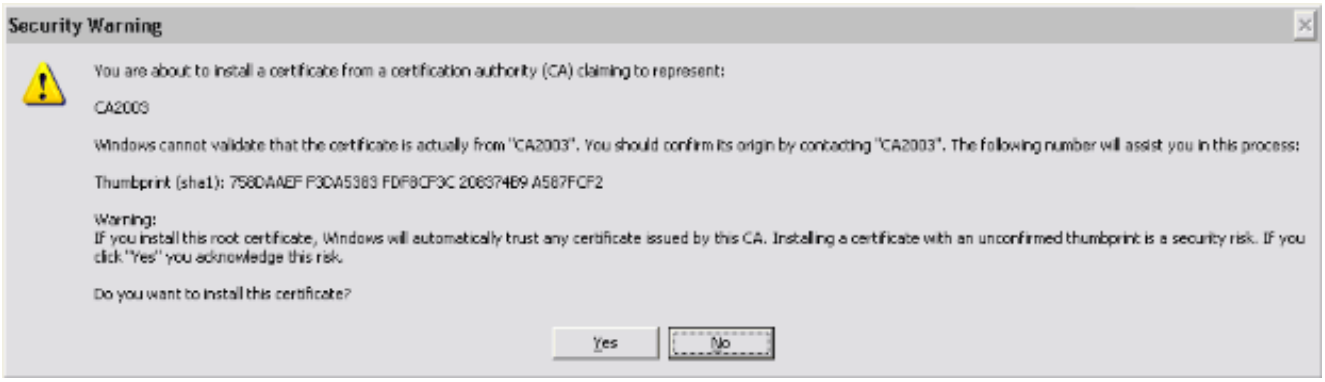
使用本部分可确认配置能否正常运行。

1. 启动AnyConnect客户端，并且连接对certenroll配置文件。

AnyConnect通过注册请求到

CA服务器SCEP。如果使用，AnyConnect直接地通过注册请求和不通过通道**获得证书**按钮。

2. 此警告出现。点击**是**安装使用用户和根证明



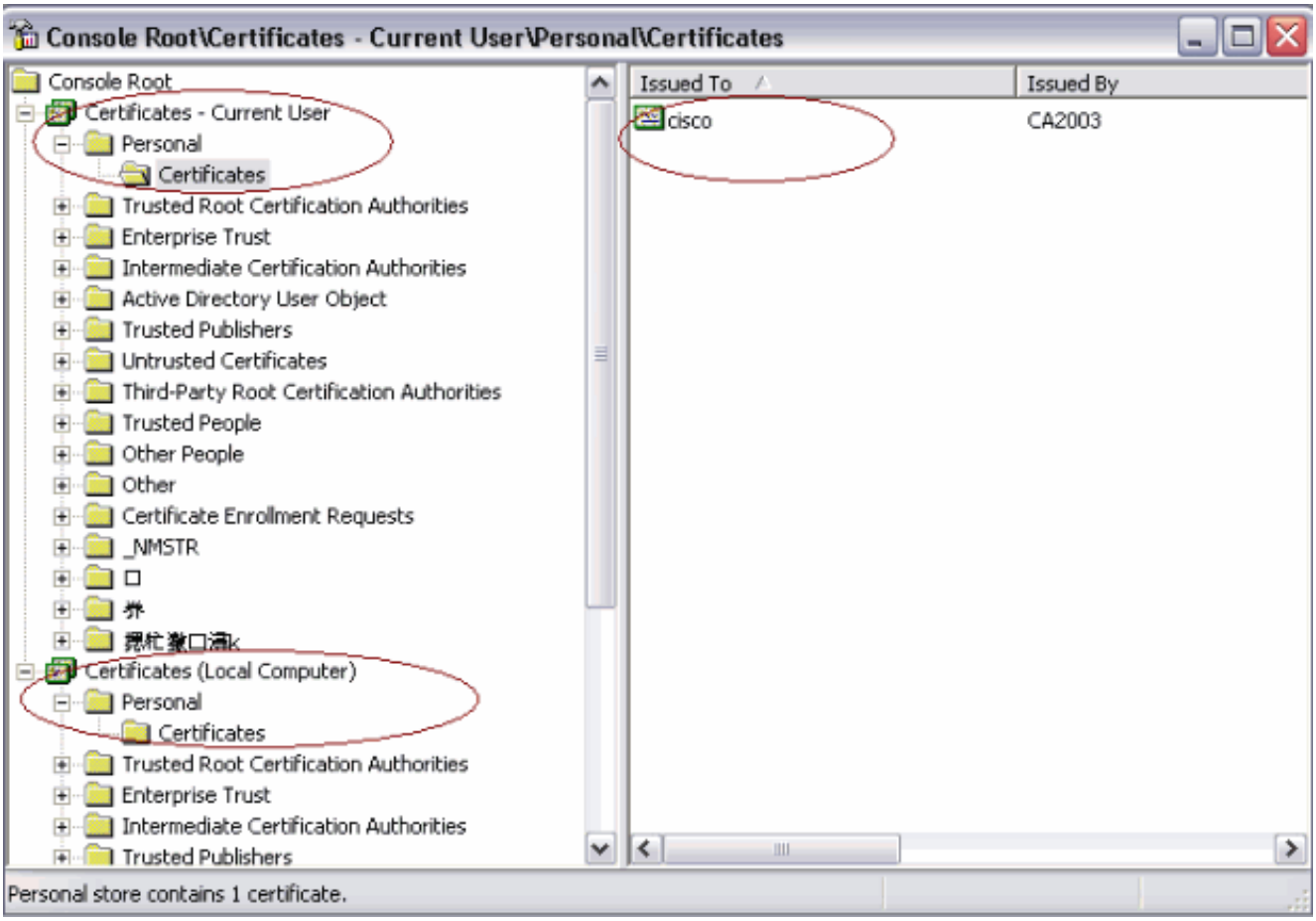
3. 一旦证书被登记，请连接对**certauth**配置文件。

在Microsoft Windows的证书存储设备在SCEP请求以后

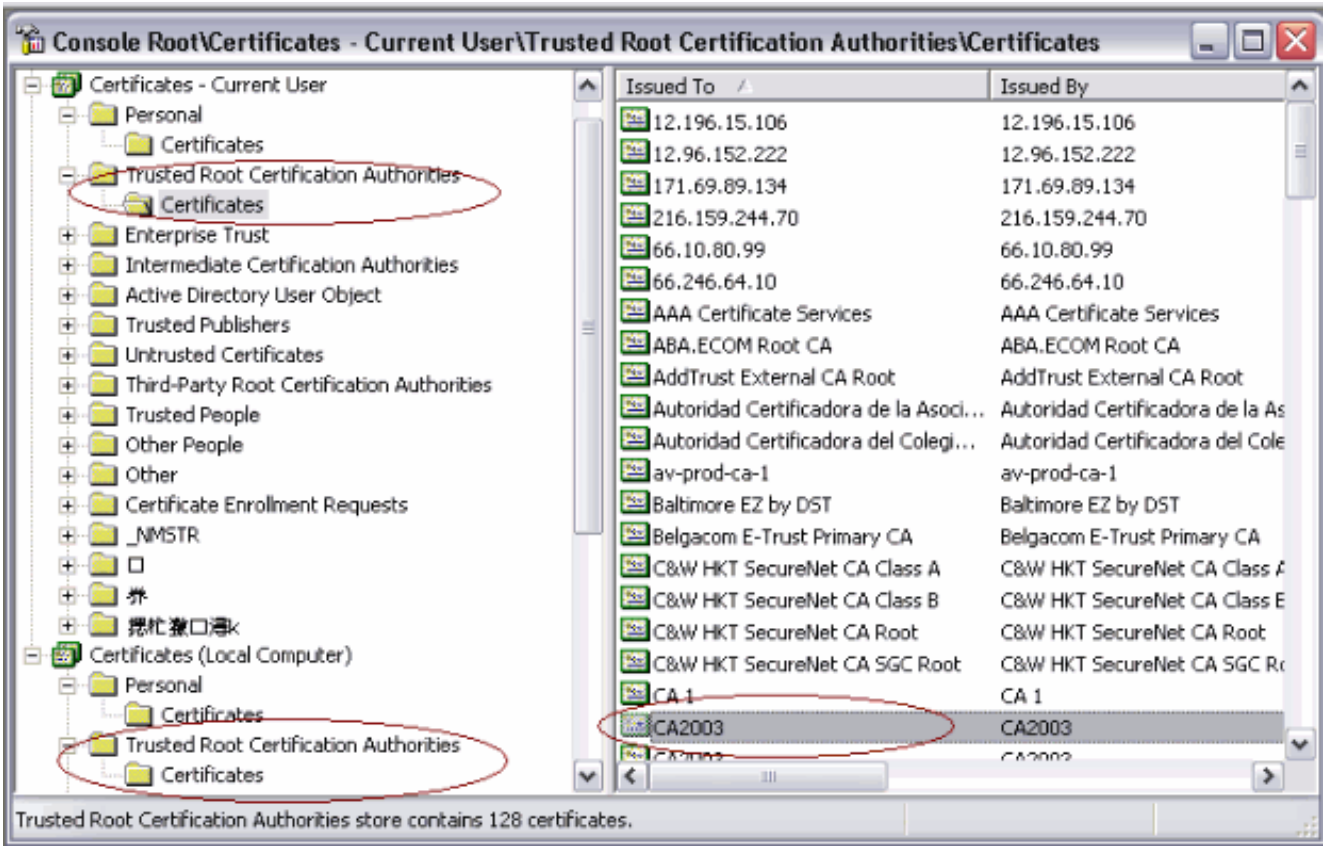
完成这些步骤：

1. 点击**Start > Run > mmc**。
2. 单击**添加/删除短冷期**。
3. 单击**添加**，并且选择**证书**。

4. 添加**我的用户帐户**和**计算机帐户**证书。此镜像显示在Windows证书存储安装的用户证书
:



此镜像显示在Windows证书存储安装的CA证书
:



故障排除

本部分提供的信息可用于对配置进行故障排除。

- 当证书验证发生故障， AnyConnect SCEP登记只运作。如果它不登记，请检查证书存储。如果证书已经安装，请删除他们并且再测试。
- 除非使用， SCEP登记不工作**ssl证书验证接口外部端口443**命令。参考这些Cisco Bug ID欲知更多信息：Cisco Bug ID CSCtf06778 (仅限注册用户) — AnyConnect SCEP登记不与每组Cert验证2一起使用Cisco Bug ID CSCtf06844 (仅限注册用户) — AnyConnect SCEP登记不工作与ASA每组Cert验证
- 如果CA服务器在ASA的外部，请确保允许与**intra-interface命令same-security-traffic的permit的**两隧道间的本地交换。如此示例所显示，并且请添加nat外部和访问列表命令：`nat (outside) 1 access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87`那里172.16.1.0 AnyConnect池和171.69.89.87是CA服务器IP地址。
- 如果CA服务器在里面，请确保包括它在**certenroll**组策略的分割隧道访问列表。在本文中，假设， CA服务器在里面。`group-policy certenroll attributes`
  `split-tunnel-policy tunnelspecified`
  `split-tunnel-network-list value scep`

  `access-list scep standard permit 171.69.89.0 255.255.255.0`

相关信息

- Cisco AnyConnect VPN客户管理员指南，版本2.4
- 技术支持和文档 - Cisco Systems