

# 配置ASA作为本地CA服务器和AnyConnect数据转发器

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[背景信息](#)

[Configure](#)

[Network Diagram](#)

[ASA作为本地CA服务器](#)

[步骤1.配置和enable \(event\)在ASA的本地CA服务器](#)

[步骤2.创建并且添加用户到ASA数据库](#)

[步骤3.在广域网接口的Enable \(event\) WebVPN](#)

[步骤4.导入在客户端机器的认证](#)

[ASA作为AnyConnect客户端的一个SSL网关](#)

[ASDM AnyConnect配置向导](#)

[配置AnyConnect的CLI](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

本文描述如何设置Cisco可适应的安全工具(ASA)作为Certificate Authority (CA)服务器和作为Cisco AnyConnect安全移动客户端的安全套接字协议层(SSL)网关。

## Prerequisites

## Requirements

Cisco 建议您了解以下主题：

- 运行软件版本9.1.x的基本的ASA配置
- ASDM 7.3或更高

## Components Used

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本9.1(6)的Cisco 5500系列ASA
- AnyConnect Windows的安全移动性客户端版本4.x

- 运行支持的OS每张[兼容性图](#)的PC。
- Cisco Adaptive Security Device Manager (ASDM)版本7.3

**Note:**请从 [Cisco 软件下载](#) 中下载 AnyConnect VPN Client 程序包 (anyconnect-win\*.pkg) ( 仅限[注册用户](#) )。将 AnyConnect VPN Client 复制到 ASA 的闪存中以供远程用户计算机下载，以便建立与 ASA 的 SSL VPN 连接。有关 ASA 配置指南的详细信息，请参阅[安装 AnyConnect 客户端](#)部分。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

## 背景信息

在ASA的认证机关提供这些功能：

- 集成在ASA的基本的认证机关操作。
- 配置证书。
- 提供安全撤销检查发出的认证。
- 在ASA提供认证机关为了用在浏览器based(WebVPN)和客户端based(AnyConnect) SSL VPN连接上。
- 提供委托数字证书给用户，不用需要取决于外部验证授权。
- 为证书验证提供一个安全，机构内部的权限和提供直接的用户登记通过网站登录。

### 指南和限制

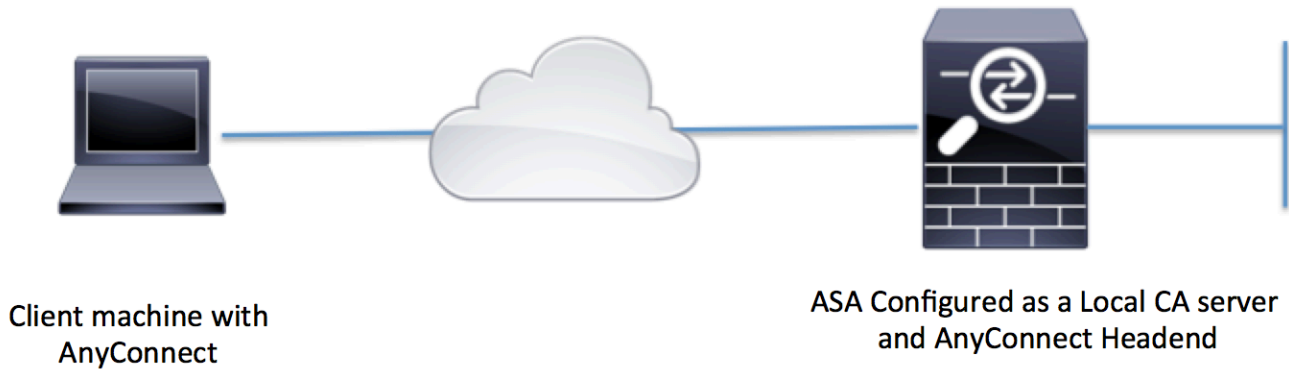
- 支持在路由的和透明防火墙模式下。
- 仅一个本地CA服务器可以每次是常驻在ASA。
- 作为本地CA服务功能故障切换设置不支持ASA。
- 作为本地CA服务器的ASA只到现在支持SHA1证书的生成。
- 本地CA服务器可以用于基于浏览器的和基于客户的SSL VPN连接。目前不支持为IPSec。
- 不支持本地CA的VPN负载均衡。
- 本地CA不可以是辅助到另一个CA。它能仅作为根CA。
- 目前ASA不能登记到本地CA身份认证的服务器。
- 当证书登记完成时，ASA存储包含用户的密钥对和证书链的一个PKCS12文件，要求大约闪存或磁盘空间2 KB每个登记。实际金额磁盘空间取决于被配置的RSA密钥大小和认证字段。请记住此指南，当添加在ASA的很大数量的待定证书登记与有限的可用闪存时，因为这些PKCS12文件在被配置的登记检索超时的期限的闪存存储。

## Configure

此部分描述如何配置Cisco ASA作为本地CA服务器。

**Note:**使用[命令查找工具](#) ( [仅限注册用户](#) ) 可获取有关本部分所使用命令的详细信息。

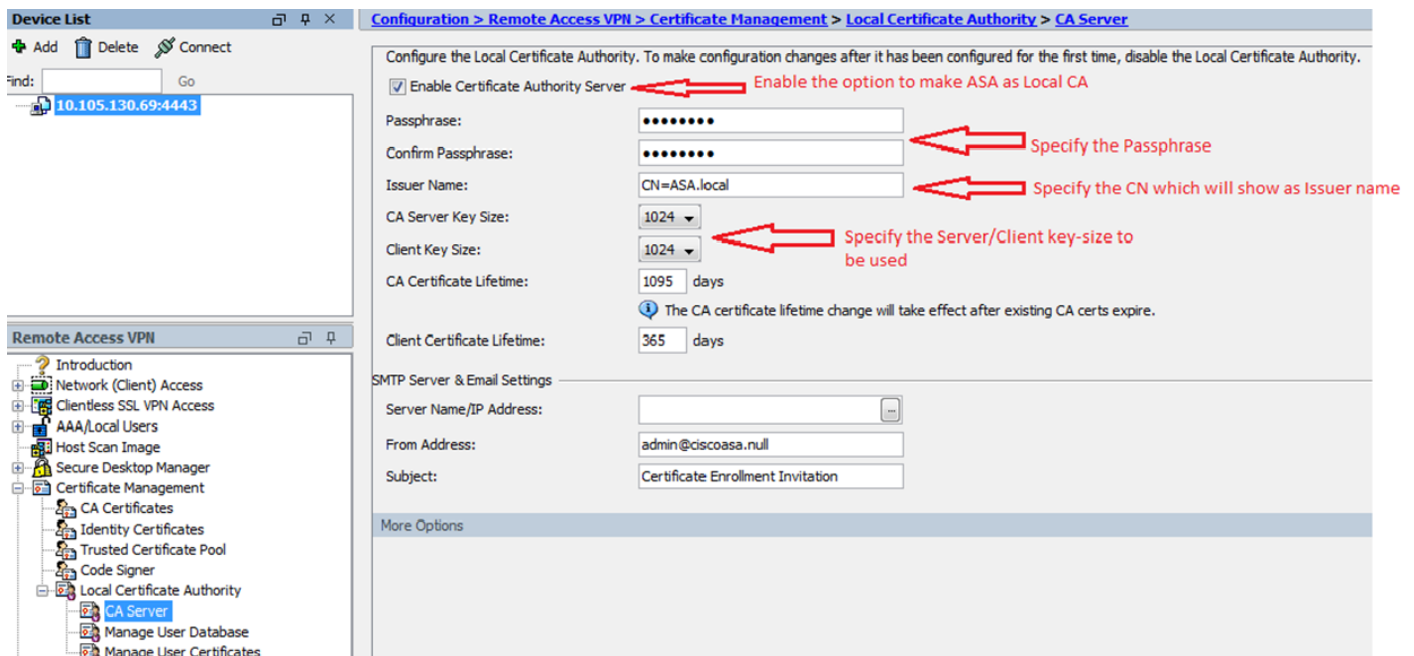
## Network Diagram



## ASA作为本地CA服务器

### 步骤1.配置和enable (event)在ASA的本地CA服务器

- 连接对**Configuration>远程访问VPN > Certificate Management >本地认证机关> CA服务器**。检查**Enable (event)认证机关服务器**选项。
- 配置密码短语。密码短语应该是用于编码和保存PKCS12文件包括本地CA证书和密钥对的最小数量，7个字符。如果CA证书或密钥对丢失，密码短语打开PKCS12档案。
- 配置发证者名字。此字段将出现作为根证明CN。这在以下格式可以指定：CN (普通的名字)，OU (组织单元)，(o)组织、L (现场)，S (状态)和C (国家)。
- **可选配置**：配置SMTP服务器，并且保证OTP的电子邮件服务器设置可能被接受通过邮件结束客户端完成登记。您可以配置您的本地Email/SMTP服务器的主机名-或IP地址。您可以从地址和客户端会收到电子邮件的主题领域也配置。默认情况下，从地址是admin@<ASA主机名->.null和主题是证书登记邀请。
- **可选配置**：您可以配置可选参数类似客户端密钥大小，CA服务器密钥大小、CA证书寿命和客户端证书寿命。



## 等效的 CLI 命令：

```
ASA(config)# crypto ca server
ASA(config-ca-server)# issuer-name CN=ASA.local
ASA(config-ca-server)# subject-name-default CN=ASA.local
ASA(config-ca-server)# lifetime certificate 365
ASA(config-ca-server)# lifetime ca-certificate 1095
ASA(config-ca-server)# passphrase cisco123
ASA(config-ca-server)# no shutdown
% Some server settings cannot be changed after CA certificate generation.
Keypair generation process begin. Please wait...
```

Completed generation of the certificate and keypair...

Archiving certificate and keypair to storage... Complete

这些是可能被配置在本地CA服务器配置下的另外的字段。

控制分配点URL	这是ASA的CRL位置。默认位置是 <a href="http://hostname.domain/+CSCOCA+/asa_ca.crl">http://hostname.domain/+CSCOCA+/asa_ca.crl</a> ，但是可能修改URL。
发布CRL接口和端口	要使CRL可以HTTP下载在一个指定接口和端口，从下拉列表请选择发布CRL接口。默认端口号是TCP端口80。
CRL寿命	本地CA更新并且补发CRL，在用户证书被取消或未撤回时候，但是，如果没有撤销更新， <b>寿命crlcommand</b> 指定在本地CA配置时的时期。如果不指定CRL寿命，默认时间是六个月。
数据库存储位置	使用本地CA数据库，ASA访问并且实现用户信息、发出的认证和撤销清单。默认情况是一个外部文件系统驻留或者可以被配置驻留。
默认主题名称	输入默认主题(DN字符串)添附到在发出的认证的用户名。允许的DN属性在此列表提供： <ul style="list-style-type: none"> <li>• CN (普通的名字) SN (姓氏)</li> <li>• O (组织名字)</li> <li>• L (现场)</li> <li>• C (国家)</li> <li>• OU (组织单位)</li> <li>• EA (电子邮件地址)</li> <li>• ST (州/省)</li> <li>• T (标题)</li> </ul>
登记期间	以内用户可能从ASA检索PKCS12文件的几小时定登记时间限制在。

DEFAULT值是24小时。

Note:如果登记期间到期，在用户检索包括用户证书的PKCS12文件前，登记没有允许。以几小时定义了时间OTP为用户登记是有效的。当用户允许登记时，此时间开始。de指定几天的数量，在认证到期前重新登记一个最初的提示被发送到认证责任人。

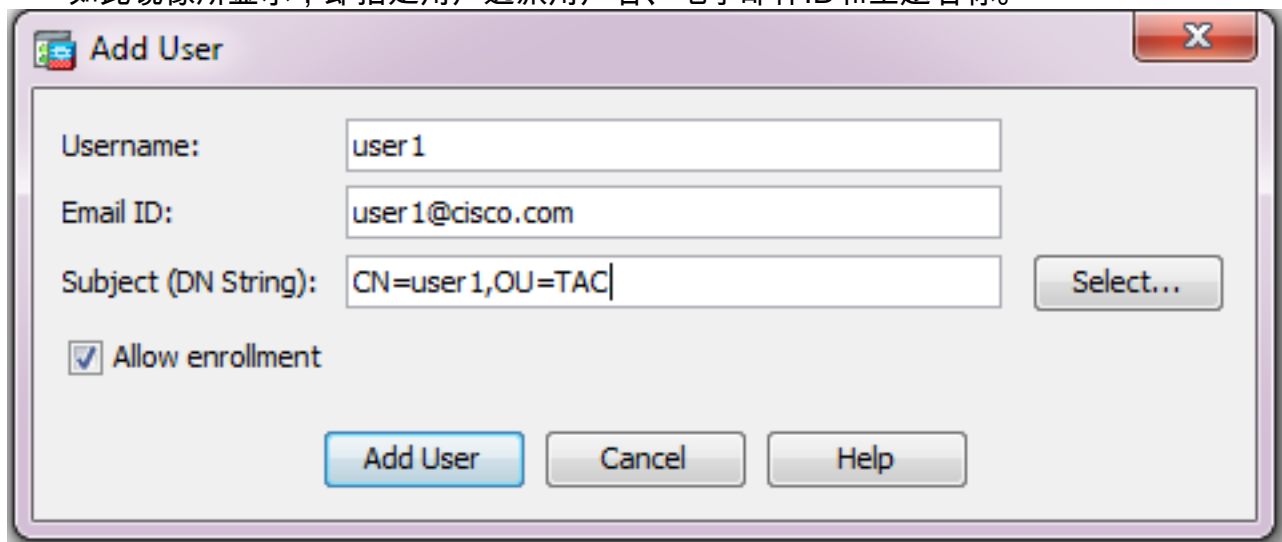
一次密码到期  
证书到期提示

## 步骤2.创建并且添加用户到ASA数据库

- 连接对Configuration>远程访问VPN > Certificate Management >本地认证机关>管理 Database.Click添加的用户。



- 如此镜像所显示，即指定用户选派用户名、电子邮件ID和主题名称。

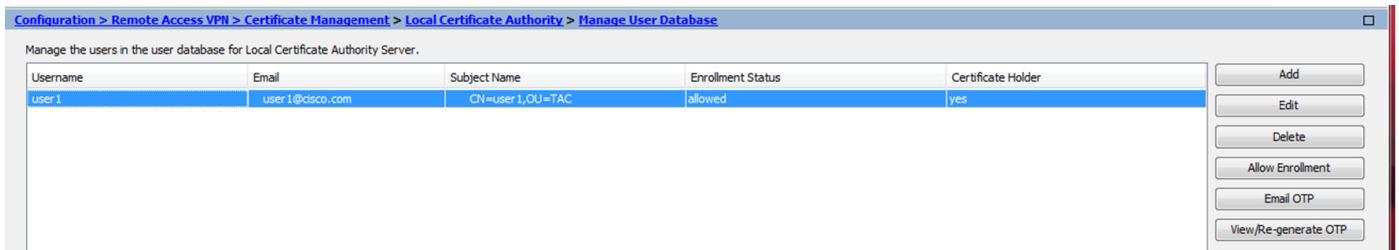


- 保证允许登记被检查，以便您允许为认证登记。
- 点击添加用户时完成用户配置。

等效的 CLI 命令：

```
ASA(config)# crypto ca server user-db add user1 dn CN=user1,OU=TAC email user1@cisco.com
```

- 在用户被添加到用户数据库后，登记状态显示如准许登记。



## 验证用户状态的CLI：

```
ASA# show crypto ca server user-db
```

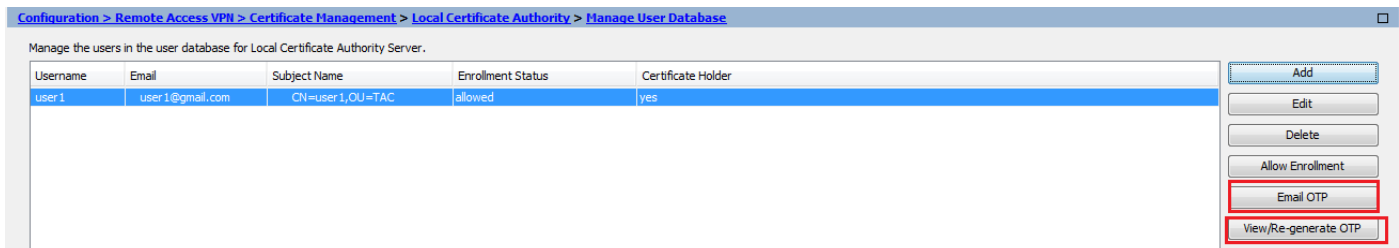
```
username: user1
email:    user1@cisco.com
dn:      CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

- 在用户被添加到了到用户数据库后，一个次密码(OTP)，用户的能完成登记，可以提供使用二者之一这：

给OTP发电子邮件(要求SMTP服务器和电子邮件设置将被配置在CA服务器配置下)。

或者

请直接地查看OTP，并且与用户的共用通过点击View/Re生成OTP。这可能也用于regenerate OTP。



## 等效的 CLI 命令：

```
ASA# show crypto ca server user-db
```

```
username: user1
email:    user1@cisco.com
dn:      CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

## 步骤3.在广域网接口的Enable (event) WebVPN

- 在ASA的Enable (event) Web访问客户端的能请求为登记。

```
ASA# show crypto ca server user-db
```

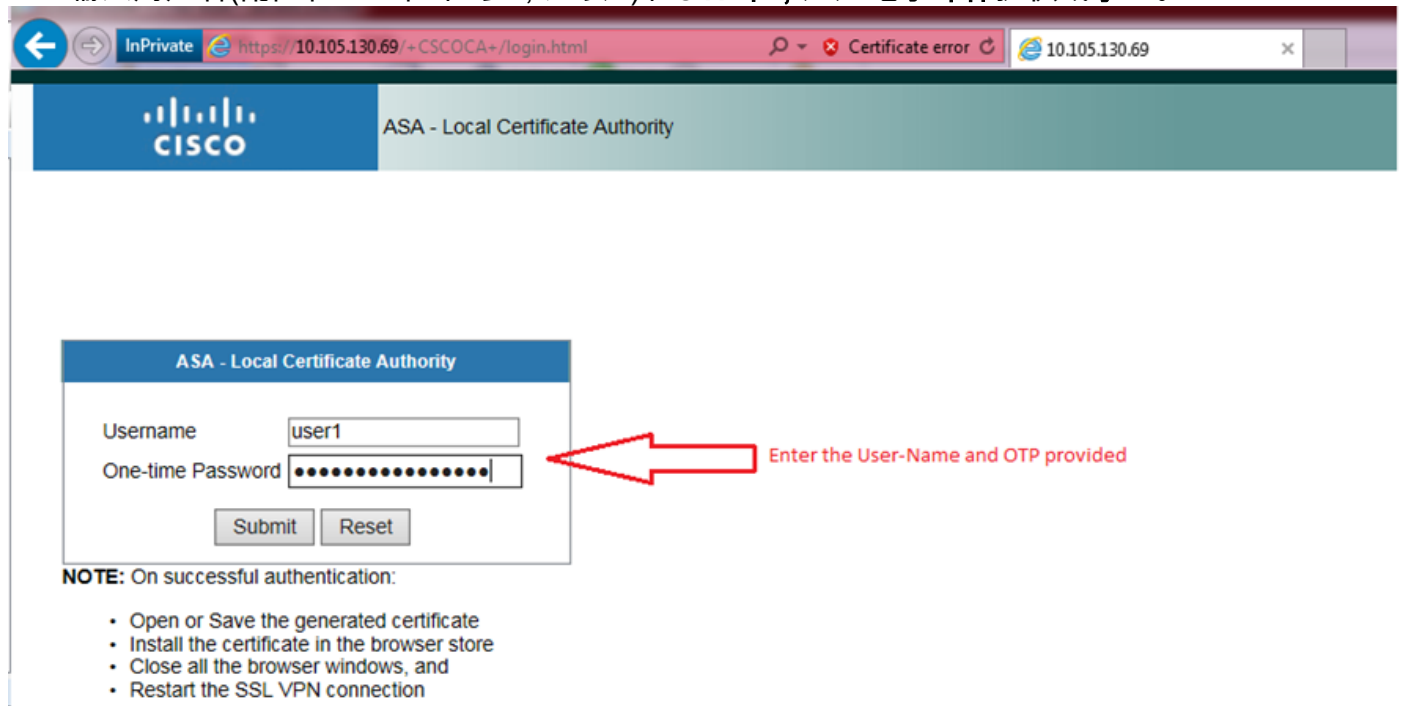
```
username: user1
email:    user1@cisco.com
dn:      CN=user1,OU=TAC
allowed: 19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

## 步骤4.导入在客户端机器的认证

- 在客户端工作站请打开浏览器并且连接对链路为了完成登记。
- 用于此链路的IP/FQDN应该是WebVPN在该步骤被启用，是接口互联网接口的IP。

<https://<ASA IP/FQDN>/+CSCOCA+/enroll.html>

- 输入用户名(配置在ASA在第2步，选项A)和OTP下，通过电子邮件提供或手工。



ASA - Local Certificate Authority

Username: user1

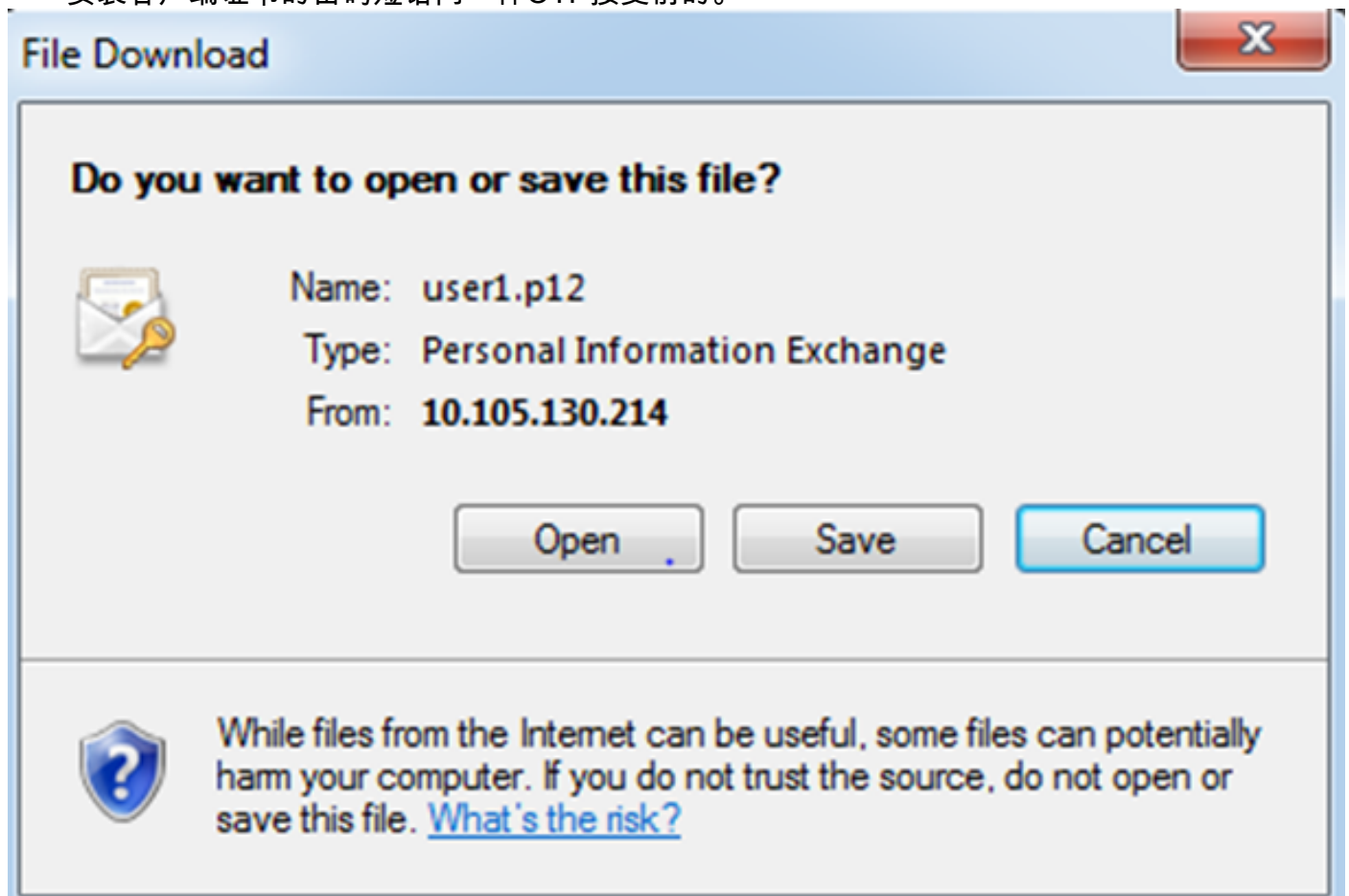
One-time Password: [Masked]

Submit Reset

**NOTE:** On successful authentication:

- Open or Save the generated certificate
- Install the certificate in the browser store
- Close all the browser windows, and
- Restart the SSL VPN connection

- 点击**开放**直接地安装从ASA接收的客户端证书。
- 安装客户端证书和密码短语同一样OTP接受前的。



File Download

Do you want to open or save this file?

Name: user1.p12

Type: Personal Information Exchange

From: 10.105.130.214

Open Save Cancel

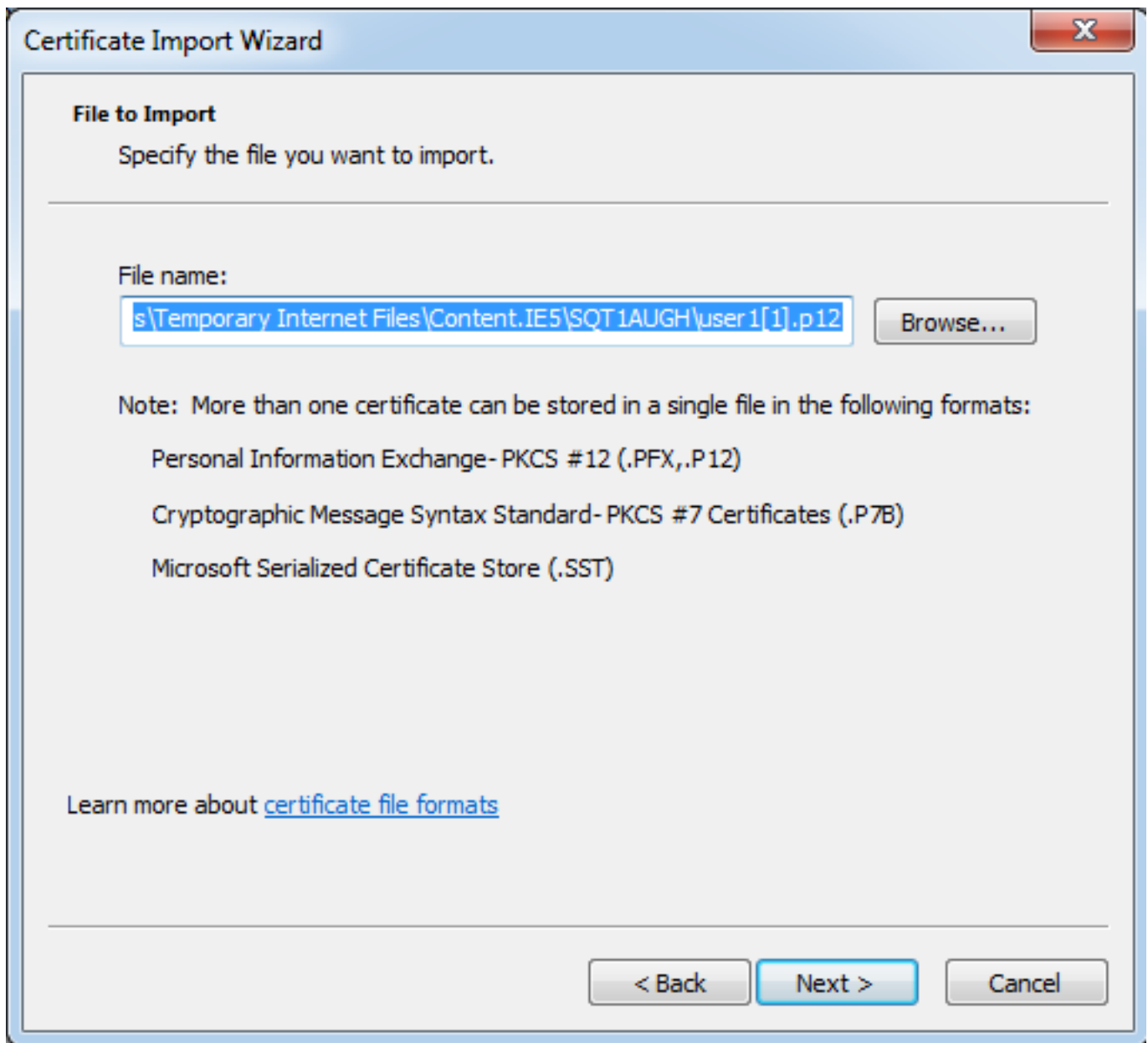
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. [What's the risk?](#)

- 单击 **Next**。

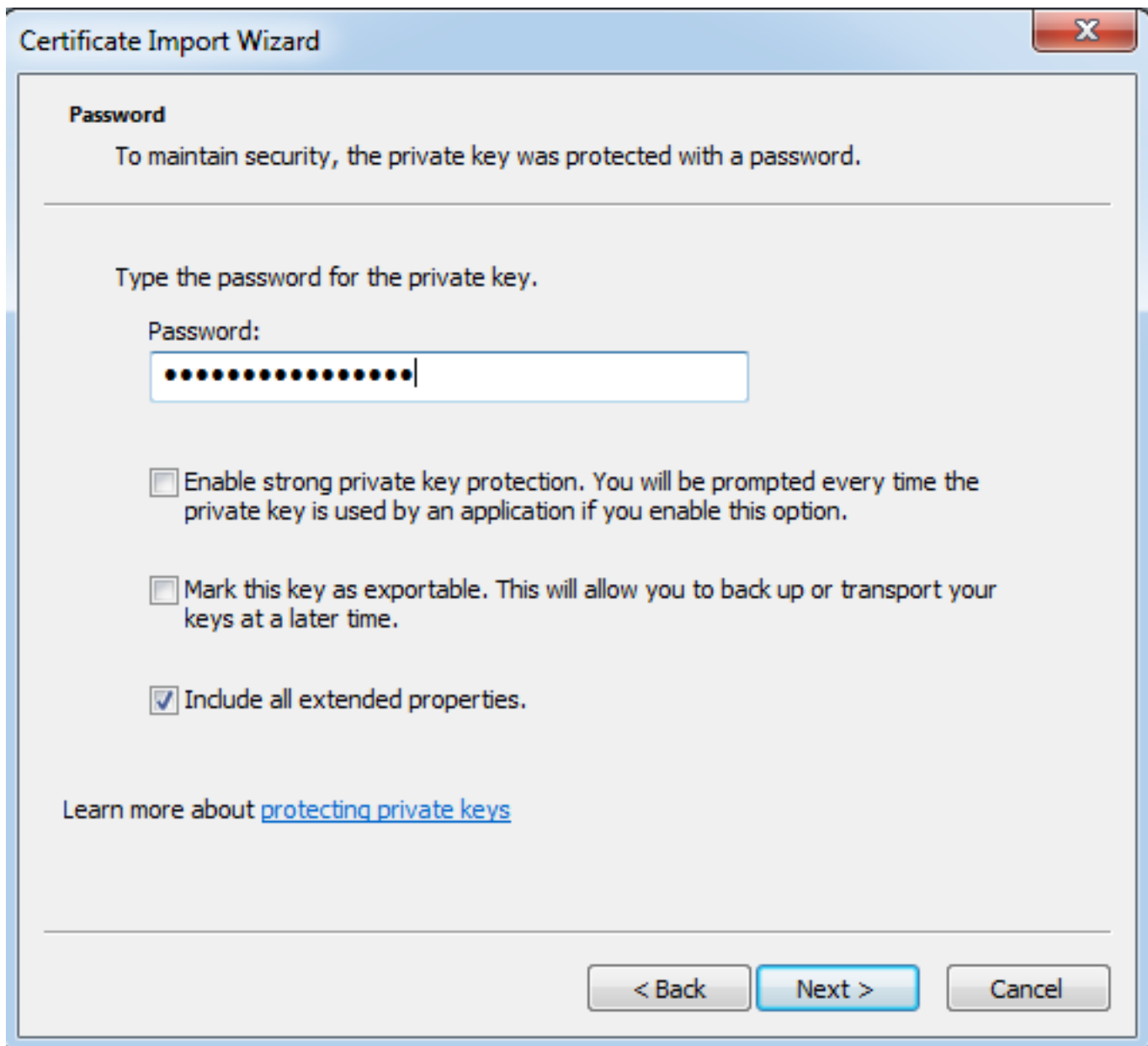


- 留下路径作为默认值并且其次点击。

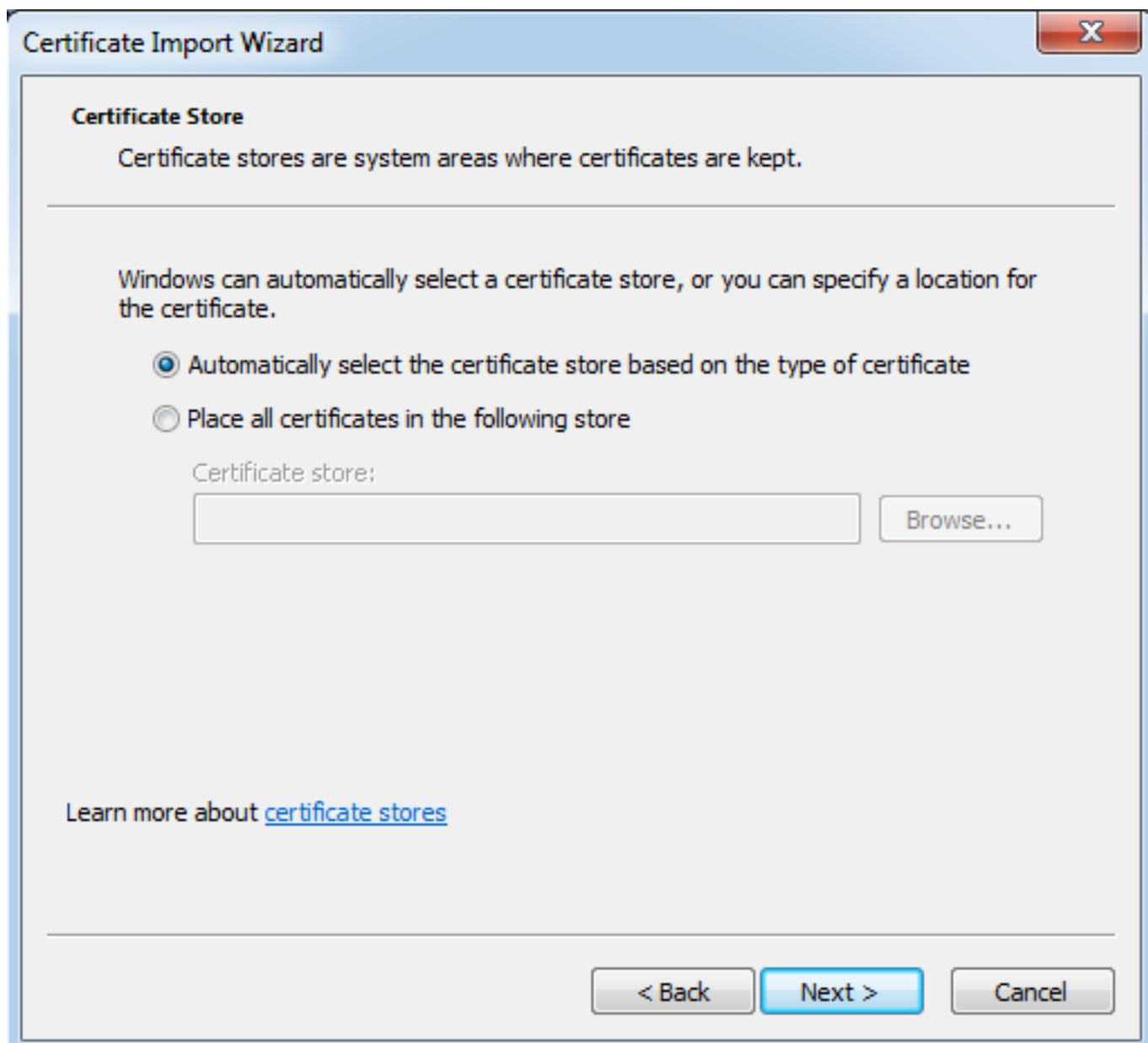




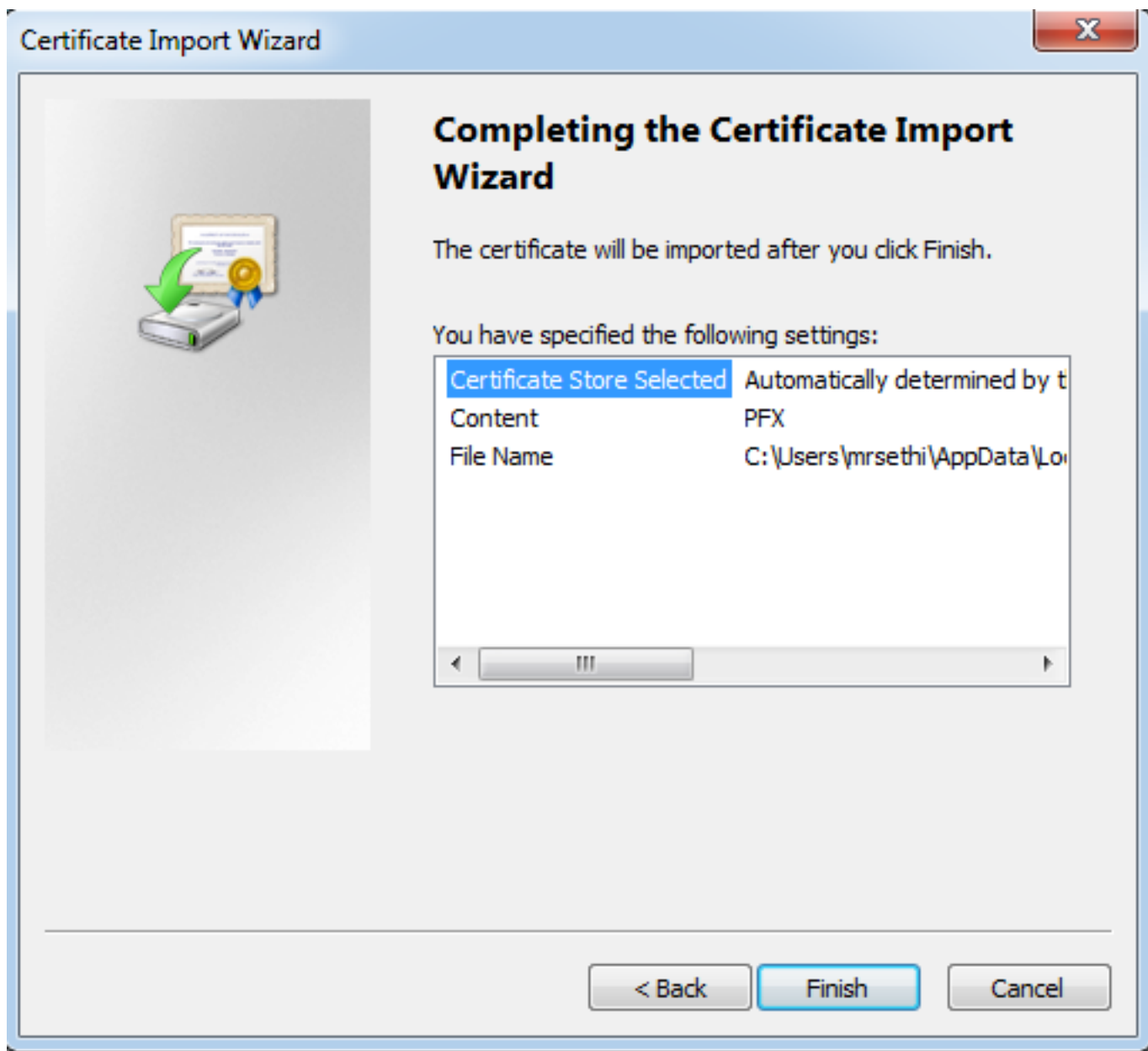
- 送进OTP在密码字段。
- 您能选择选项指示此键如可输出，以便键能从工作站如果必须被导出今后。
- 其次点击



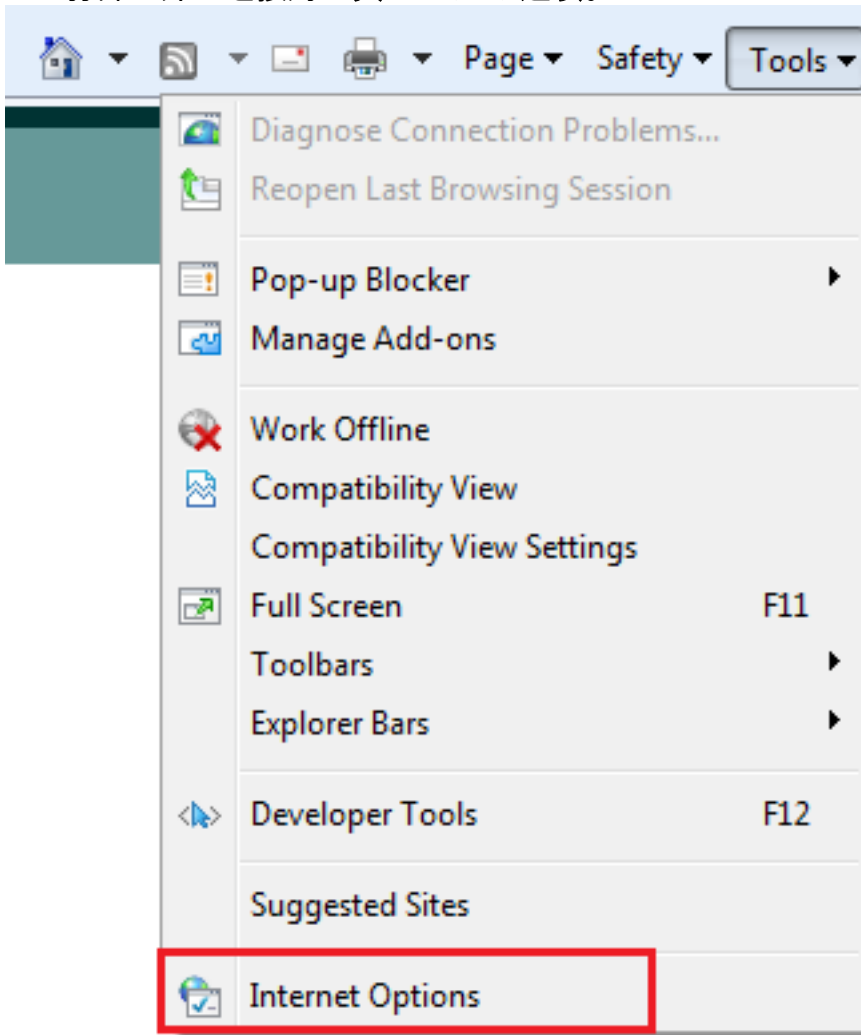
- 您能在一定的证书存储上手工安装认证或留下它自动地选择存储。
- 单击 **Next**。



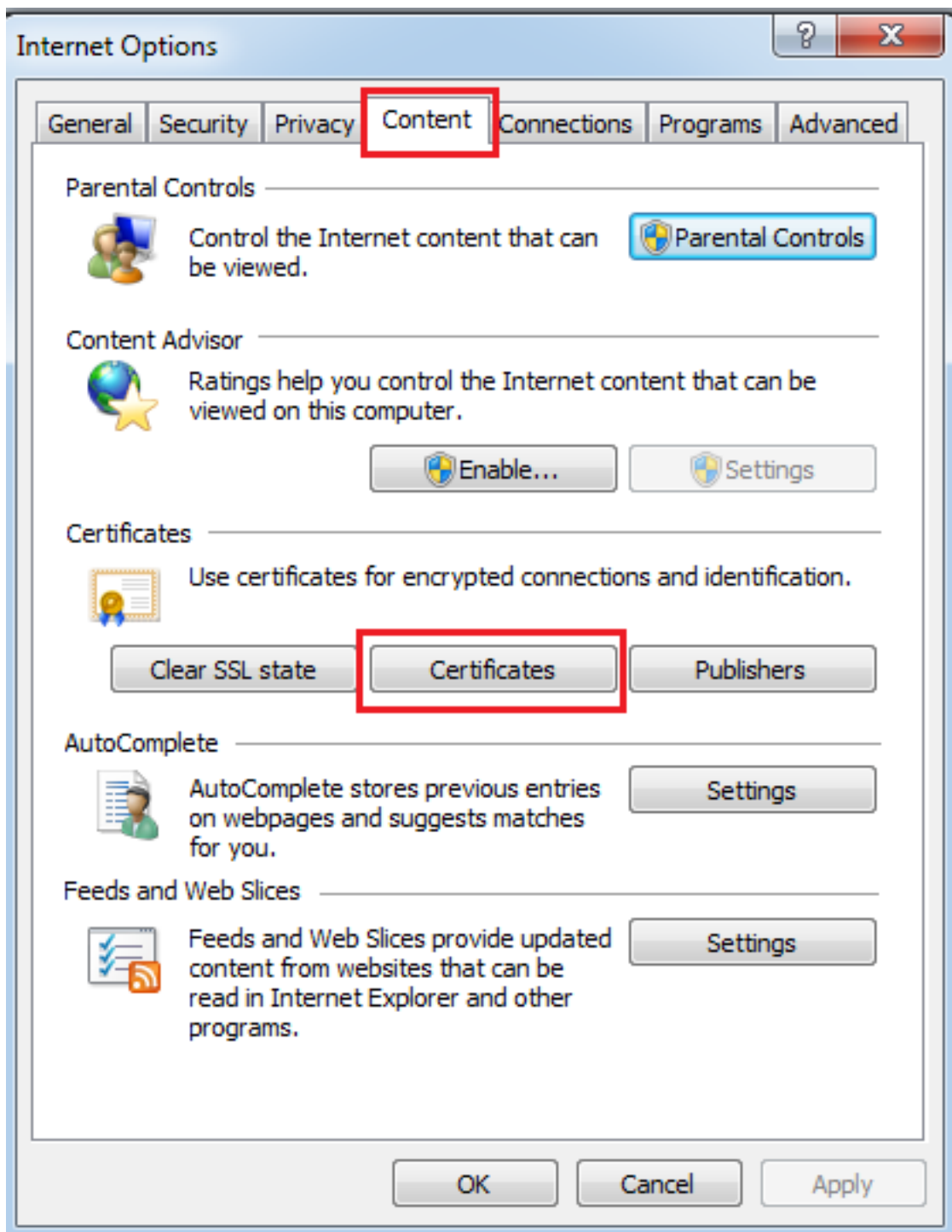
- 点击**完成**为了完成安装。



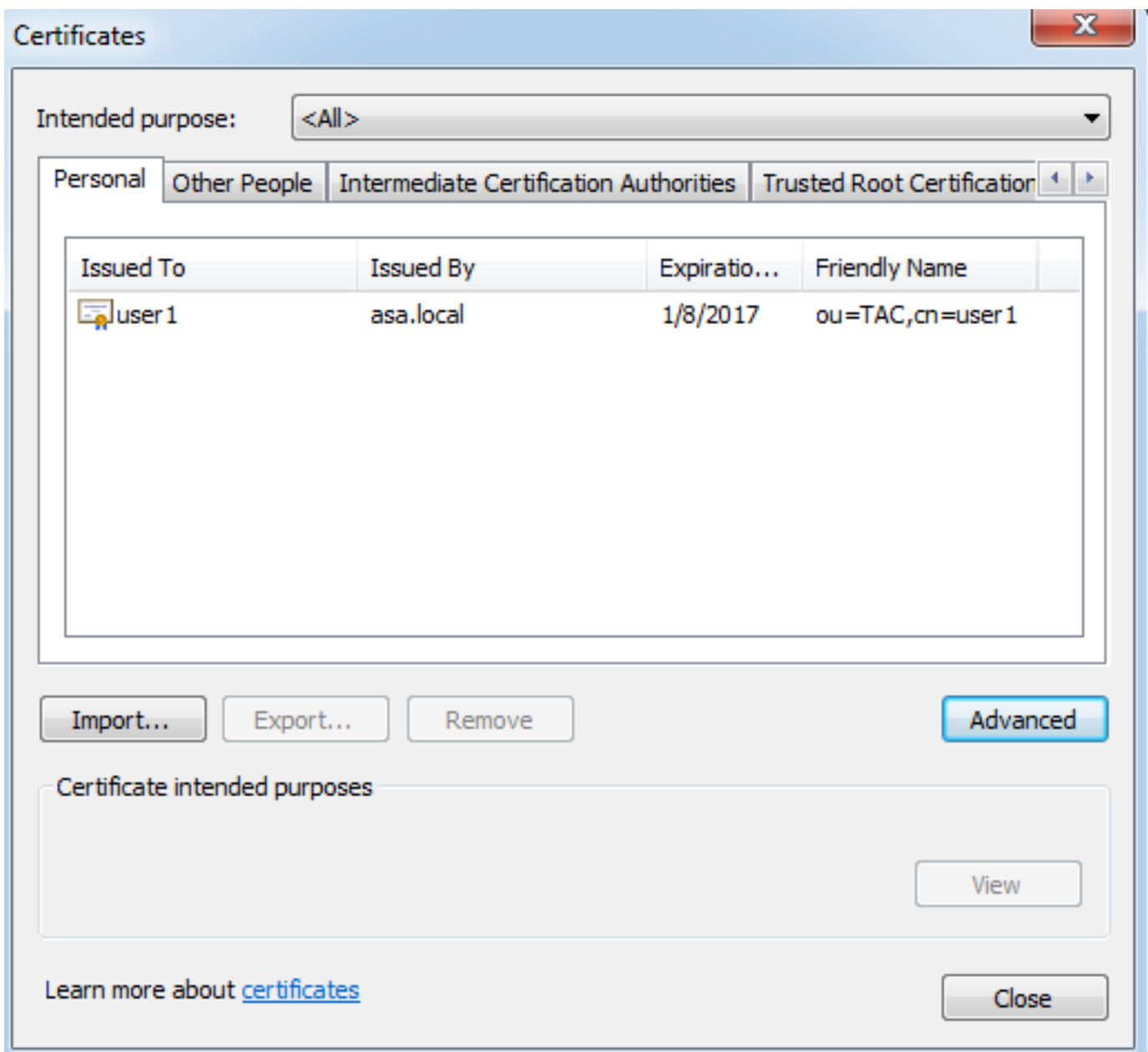
- 一旦成功安装认证，您能验证它。
- 打开IE并且连接对**工具> Internet选项**。



- 如此镜像所显示，连接使选项满意并且点击**证书**。



- 在私有存储下，您能看到从ASA接收的认证。



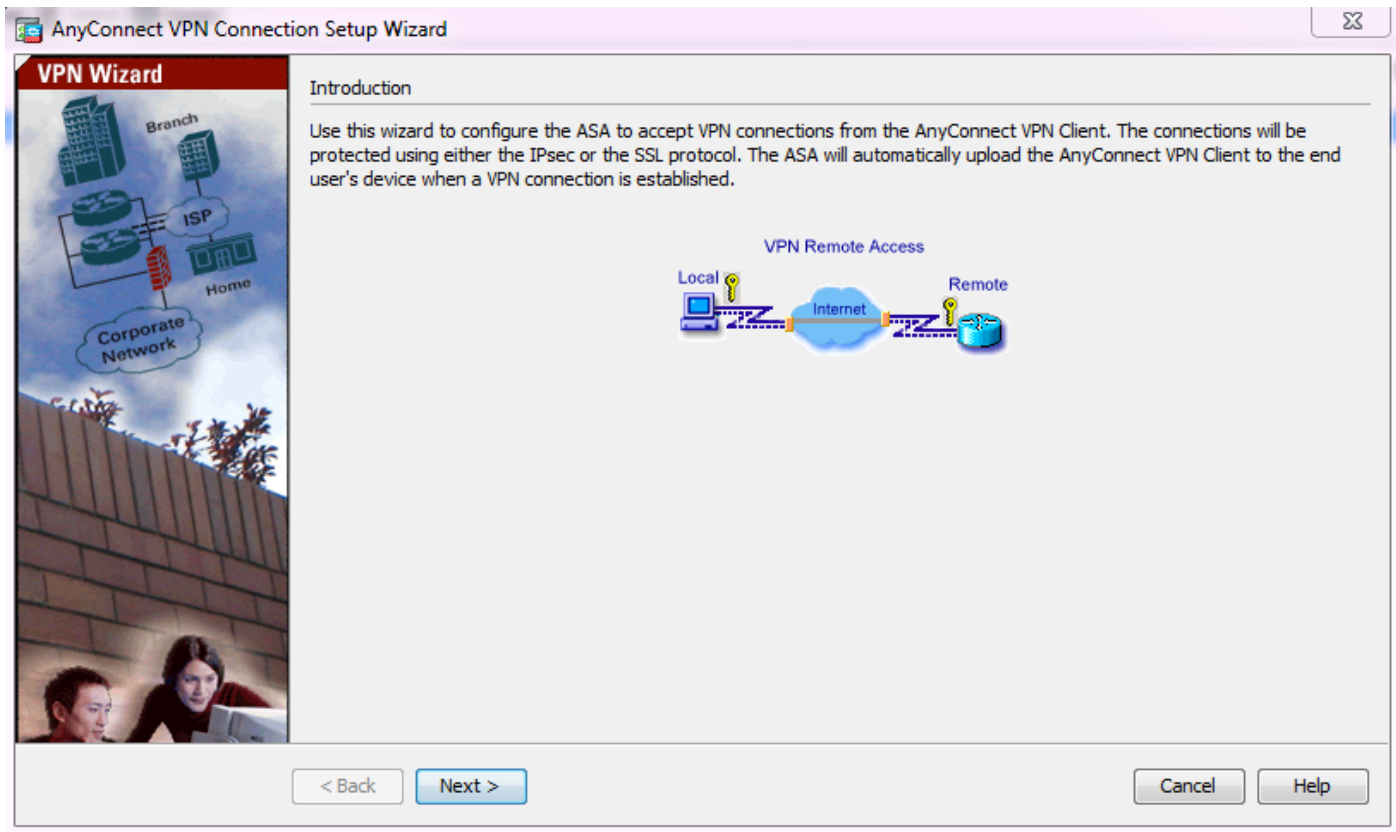
## ASA作为AnyConnect客户端的SSL网关

### ASDM AnyConnect配置向导

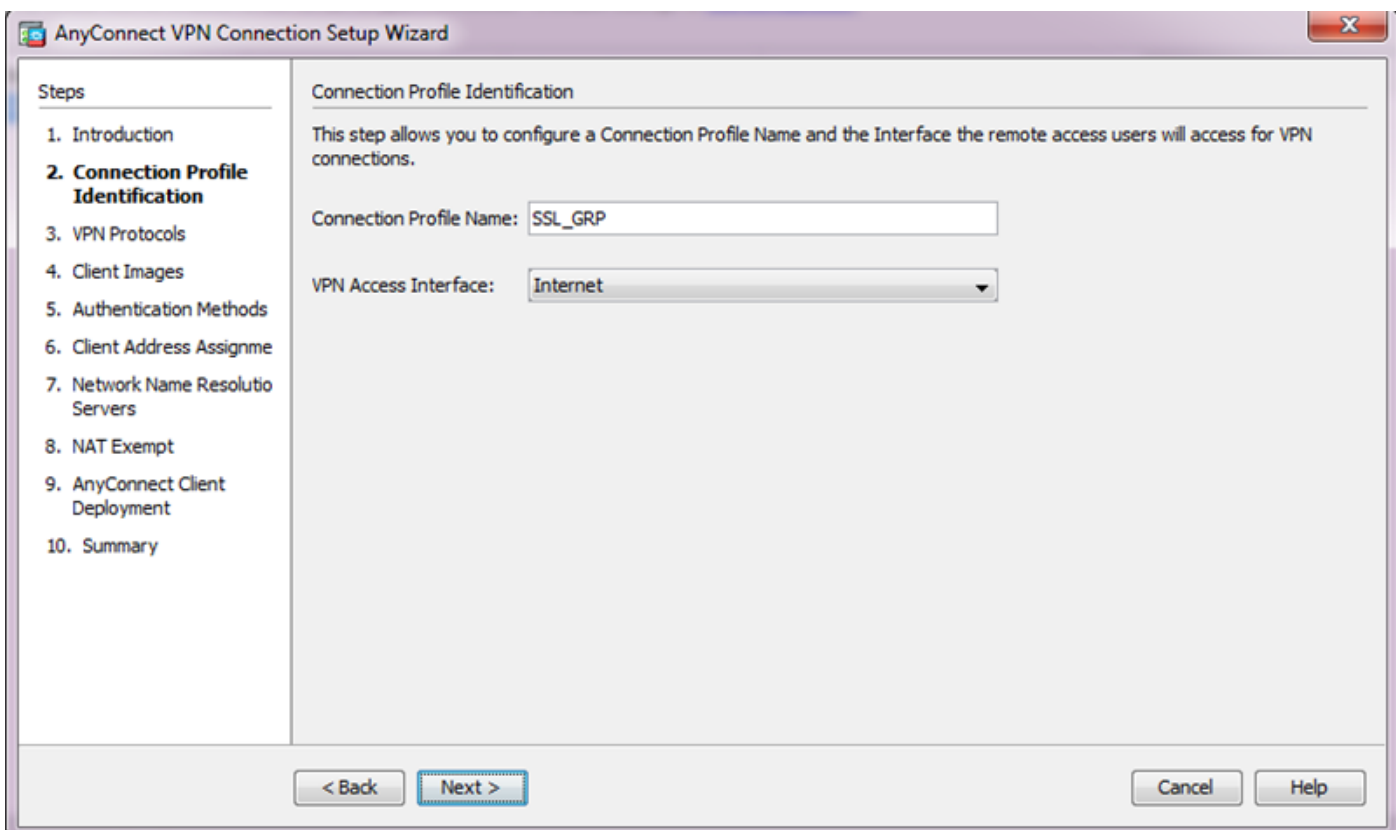
AnyConnect配置Wizard/CLI可以用于为了配置AnyConnect安全移动性客户端。保证AnyConnect客户端程序包被加载了到ASA防火墙的闪存/磁盘，在您进行前。

完成这些步骤为了通过配置向导配置AnyConnect安全移动性客户端：

1. 日志到ASDM里和连接到启动配置向导的Wizards> VPN向导> AnyConnect VPN向导并且其次点击。



2. 输入连接配置文件名字，选择VPN从VPN访问接口下拉菜单将被终止的接口，并且其次点击。

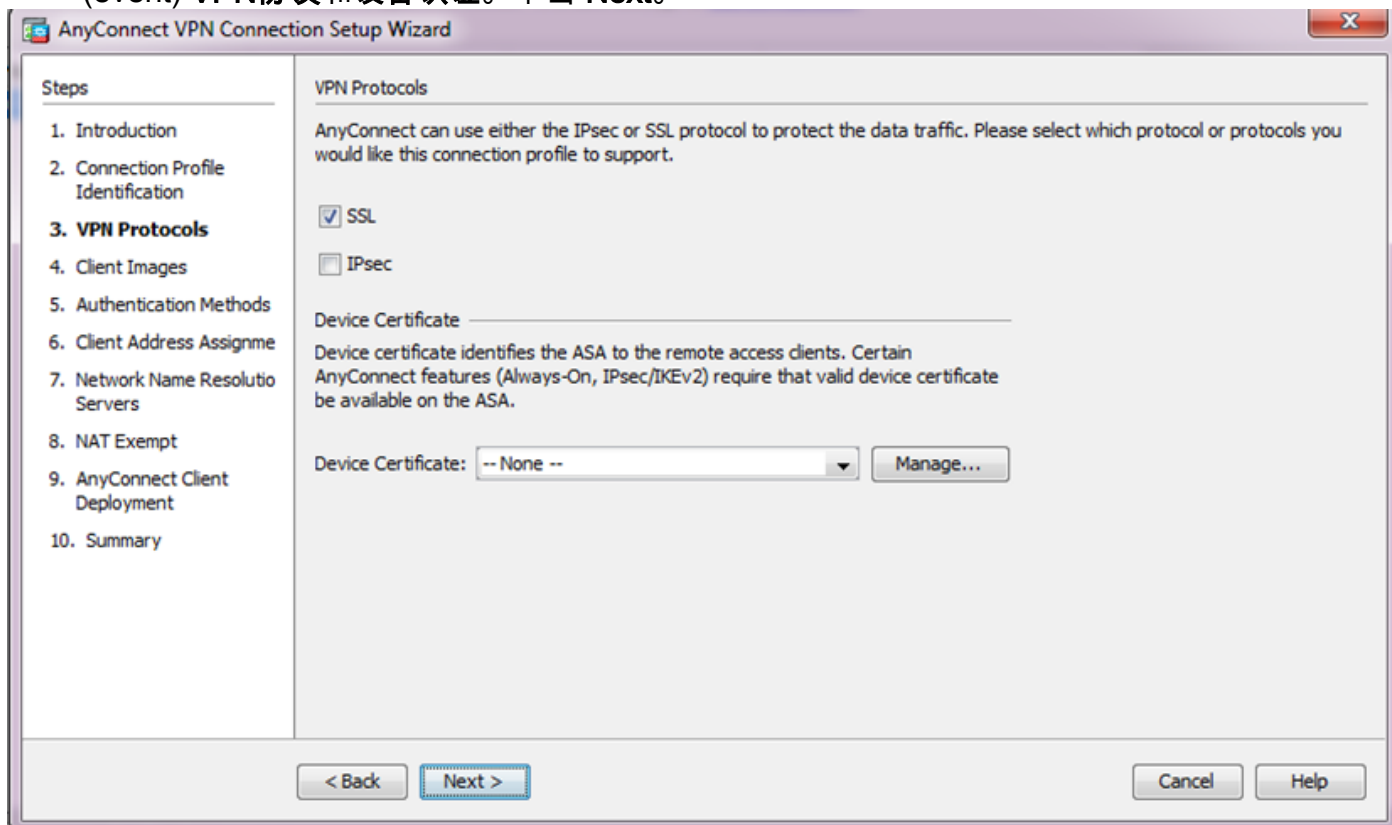


3. 检查SSL复选框为了enable (event)安全套接字协议层(SSL)。设备认证可以是一个委托的第三方 Certificate Authority (CA)发出的认证(例如Verisign或者Entrust)，或者自签证书。如果认证在ASA上已经安装，则可以通过下拉菜单被选择。

1. **Note:**此认证是将由ASA提交给SSL客户端的服务器端认证。如果比必须生成没有在ASA上当前安装的服务器证明自签证书，则请点击**管理**。为了安装一个第三方认证，请完成在[ASA](#)

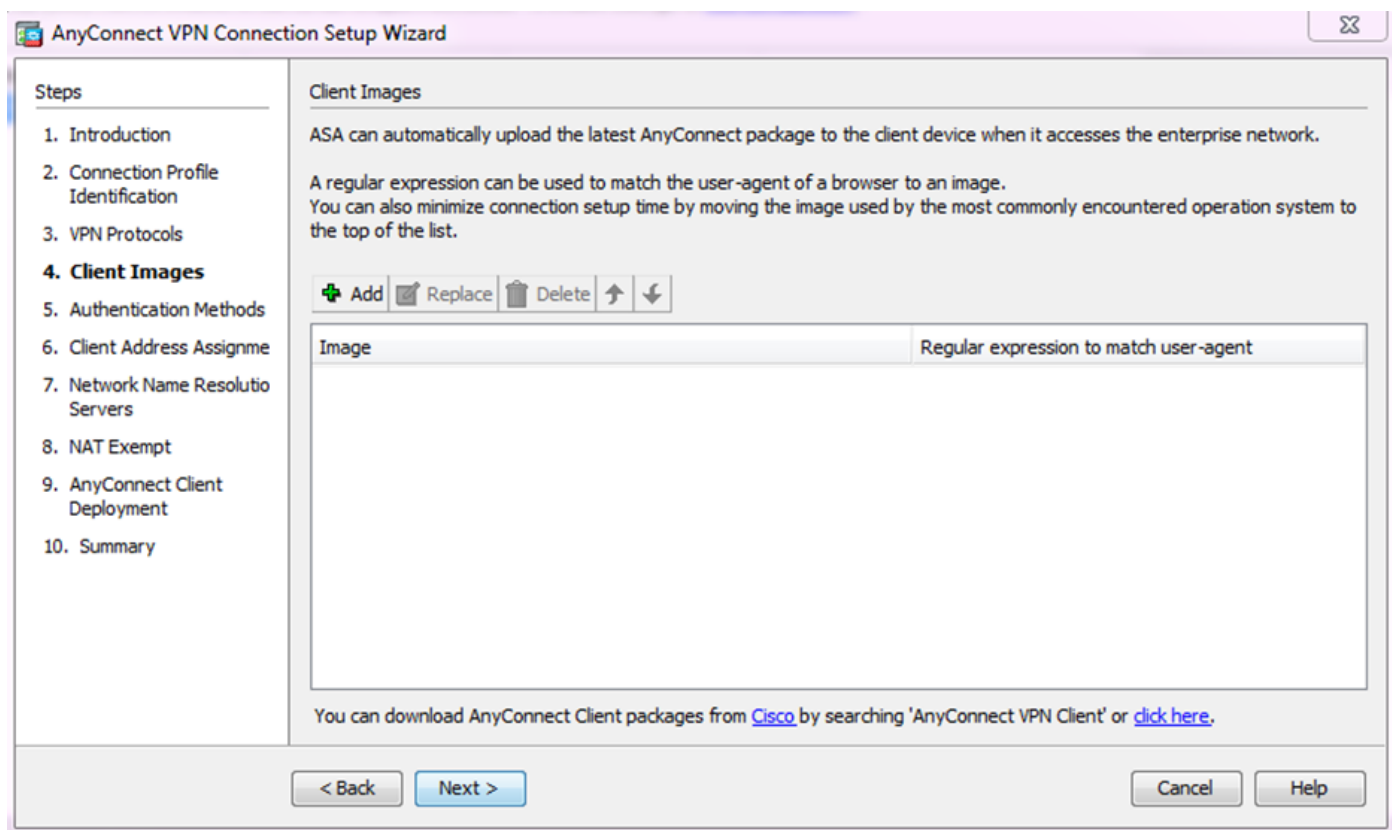


8.x描述手工安装第三方供应商证书为了用在WebVPN配置示例Cisco文档上的步骤。Enable (event) VPN协议和设备认证。单击 Next。



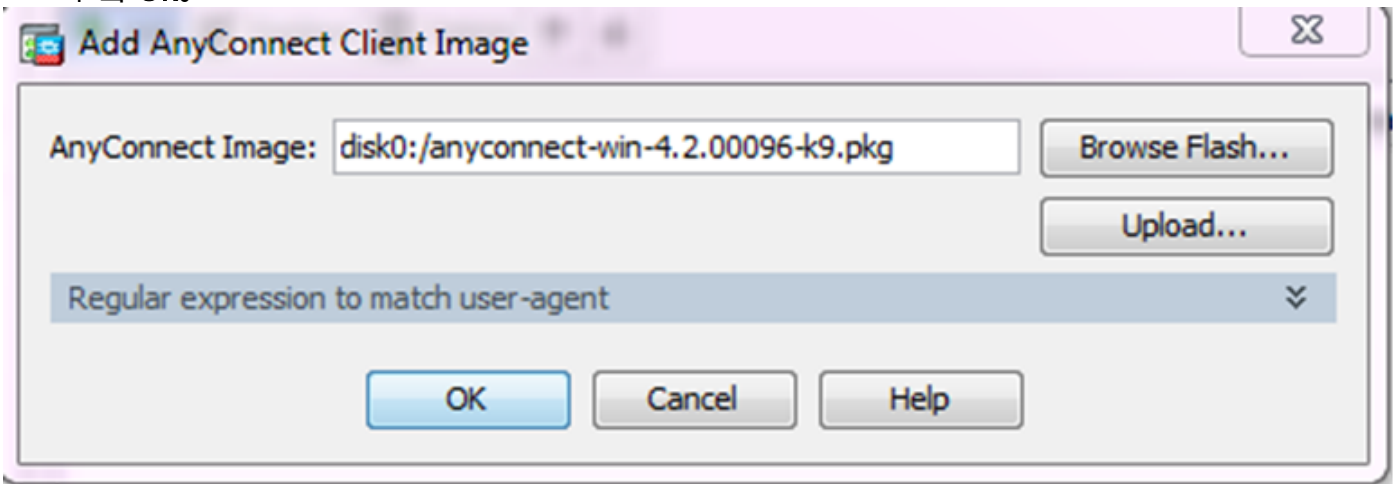
4. 点击添加为了添加AnyConnect客户端程序包(.pkg文件)从本地驱动器或从ASA闪存/磁盘。

点击访问闪存为了从闪存驱动器添加镜像或者点击加载为了从主机本地驱动器添加镜像。

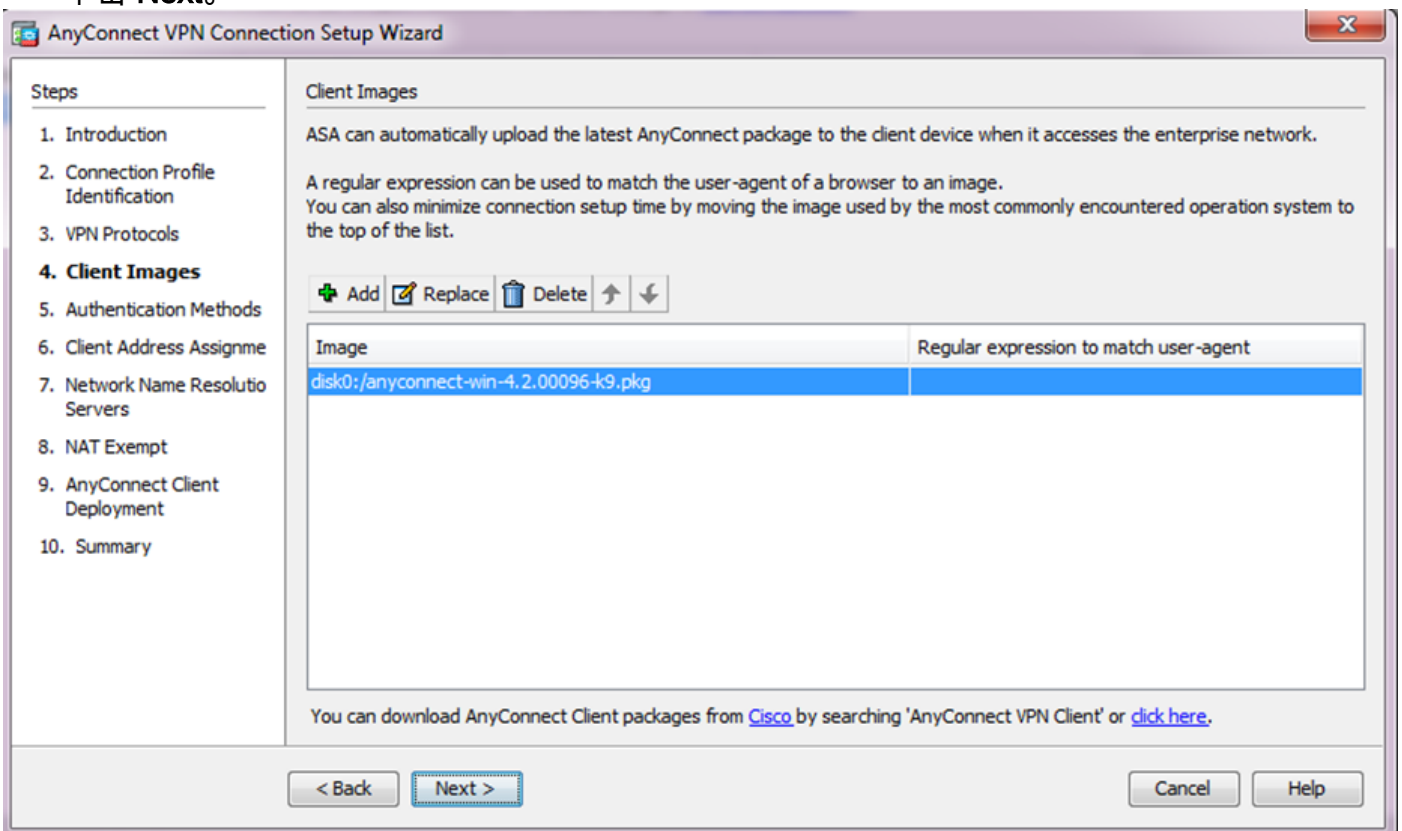


- 您可能从ASA闪存加载AnyConnect.pkg文件/磁盘(如果程序包已经是那里)或从本地驱动器。
- 访问闪存-从ASA闪存/磁盘选择AnyConnect程序包。

- 加载-选择AnyConnect程序包从主机本地驱动器。
- 单击 Ok。

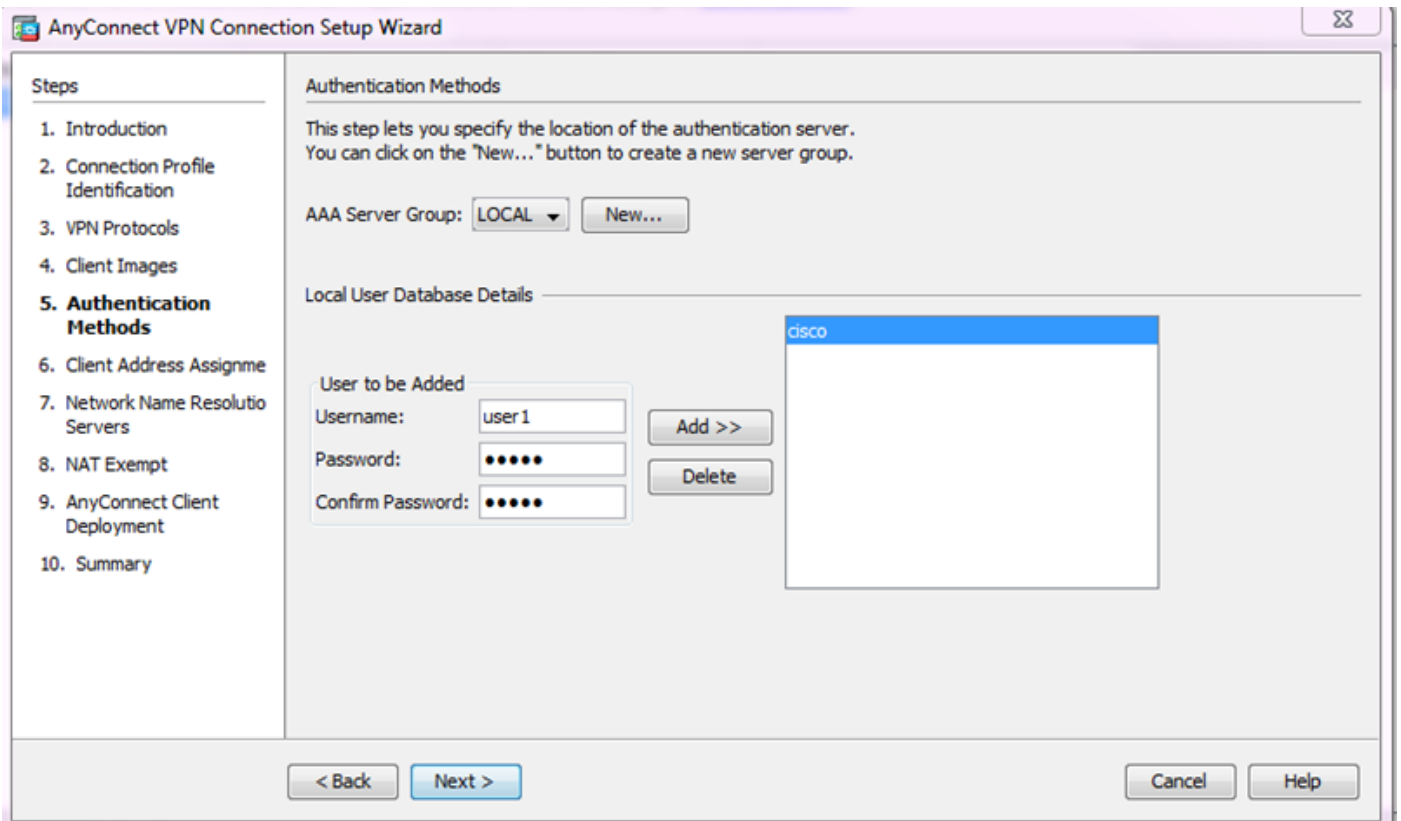


- 单击 Next。

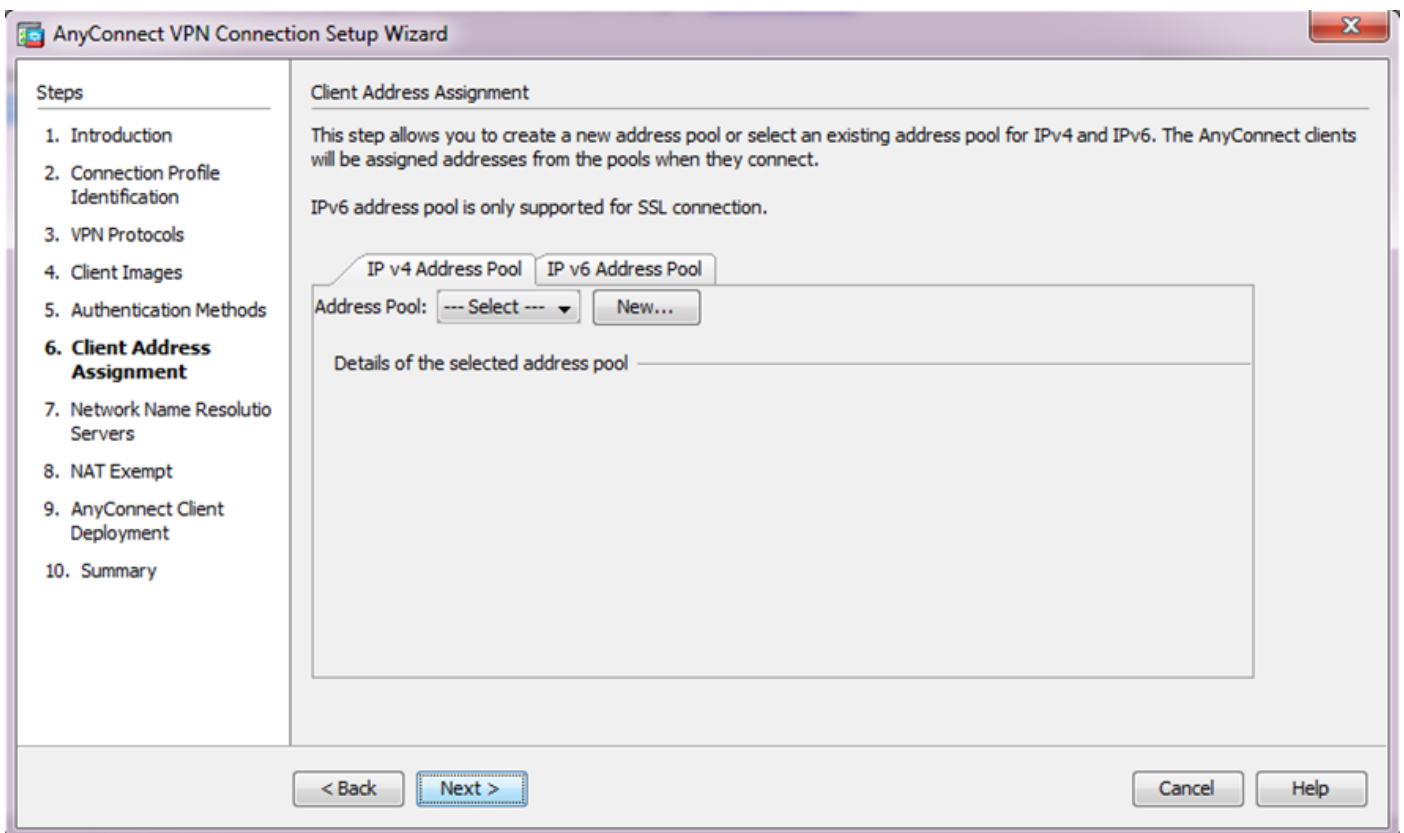


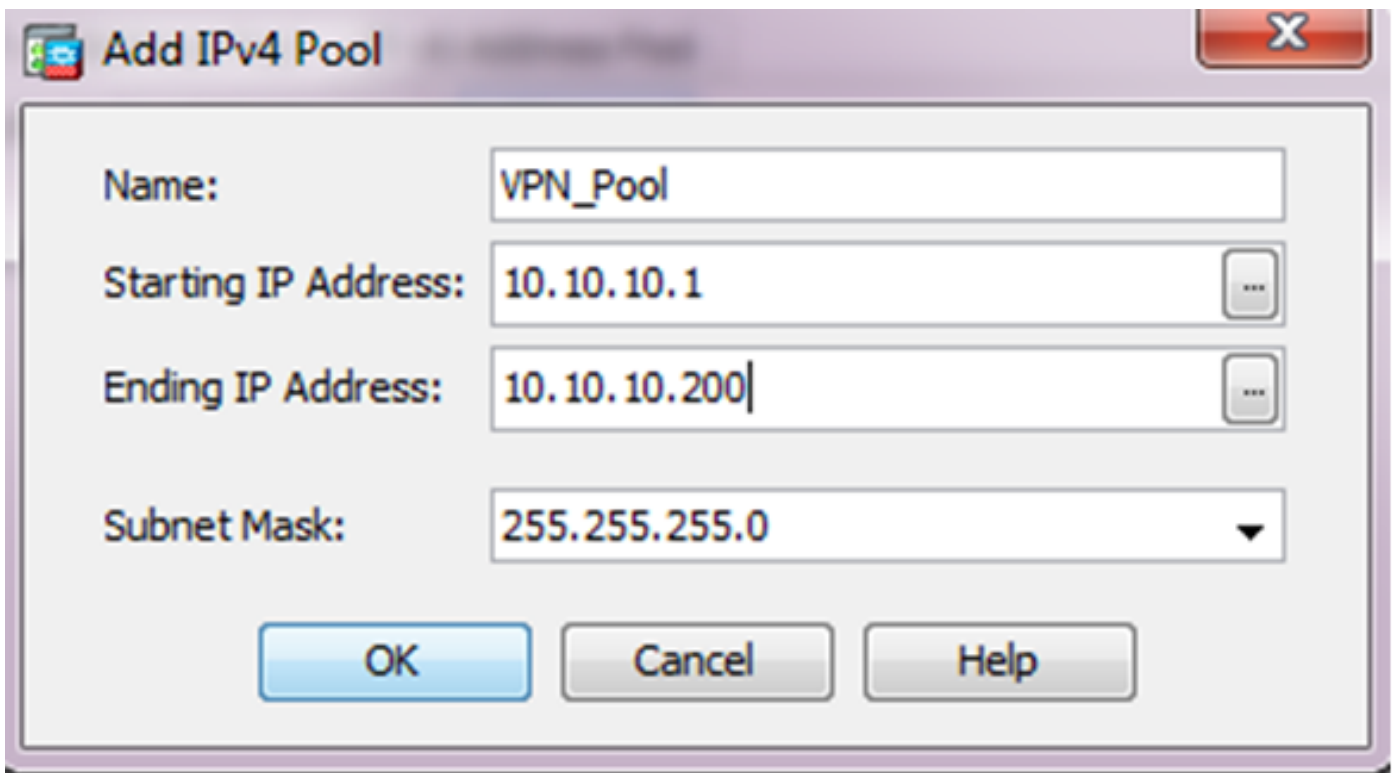
5. 用户认证可以通过验证、授权和统计(AAA)服务器组完成。如果已经配置用户，则请选择本地并且其次点击。请添加一个用户到本地用户数据库并且其次点击。

**Note:**在本例中，配置本地认证，因此意味着在ASA的本地用户数据库将使用认证。

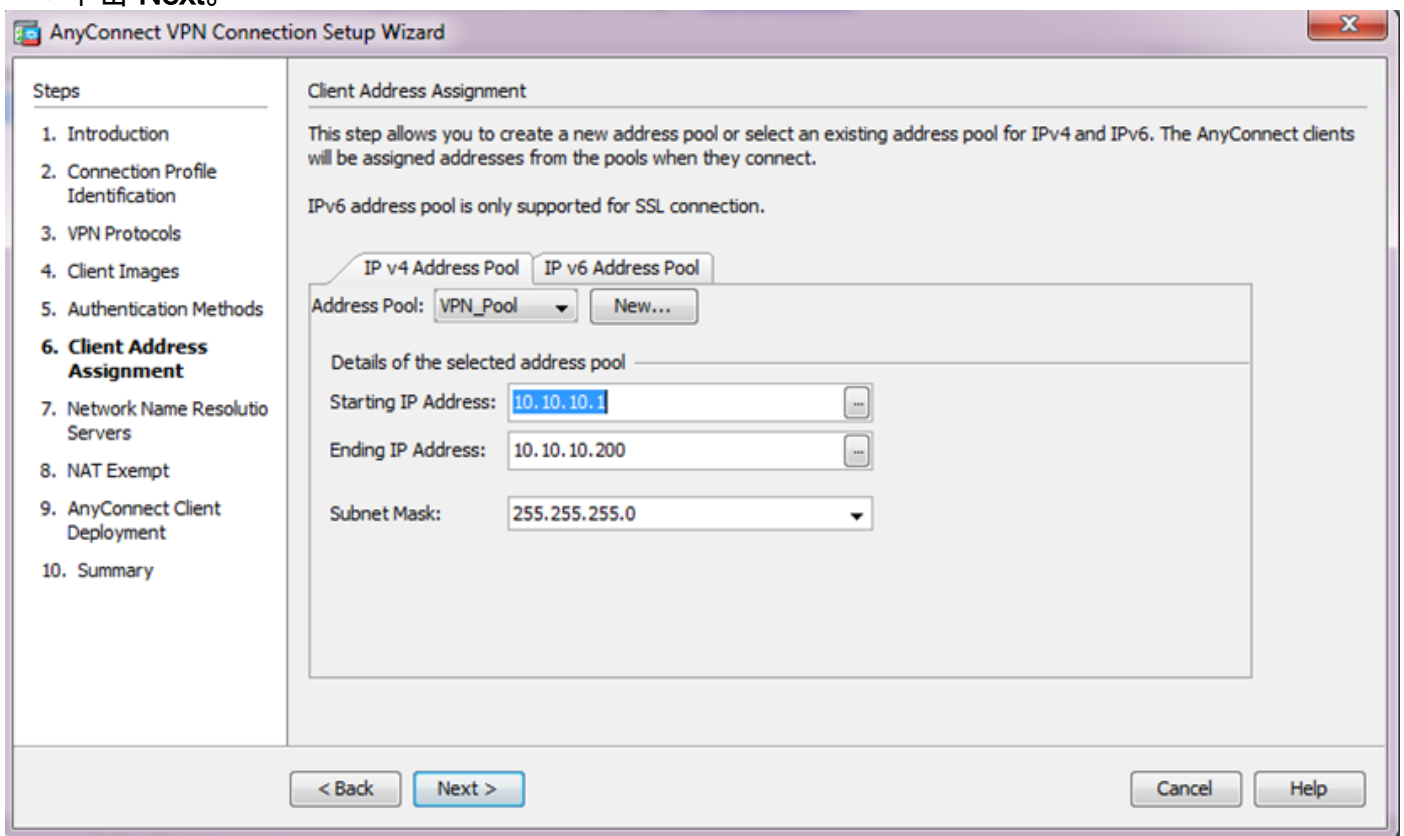


6. 保证配置VPN客户端的地址池。如果那么已经配置得IP池请选择它从下拉菜单。否则，请点击新为了配置。一旦完全，其次请点击。

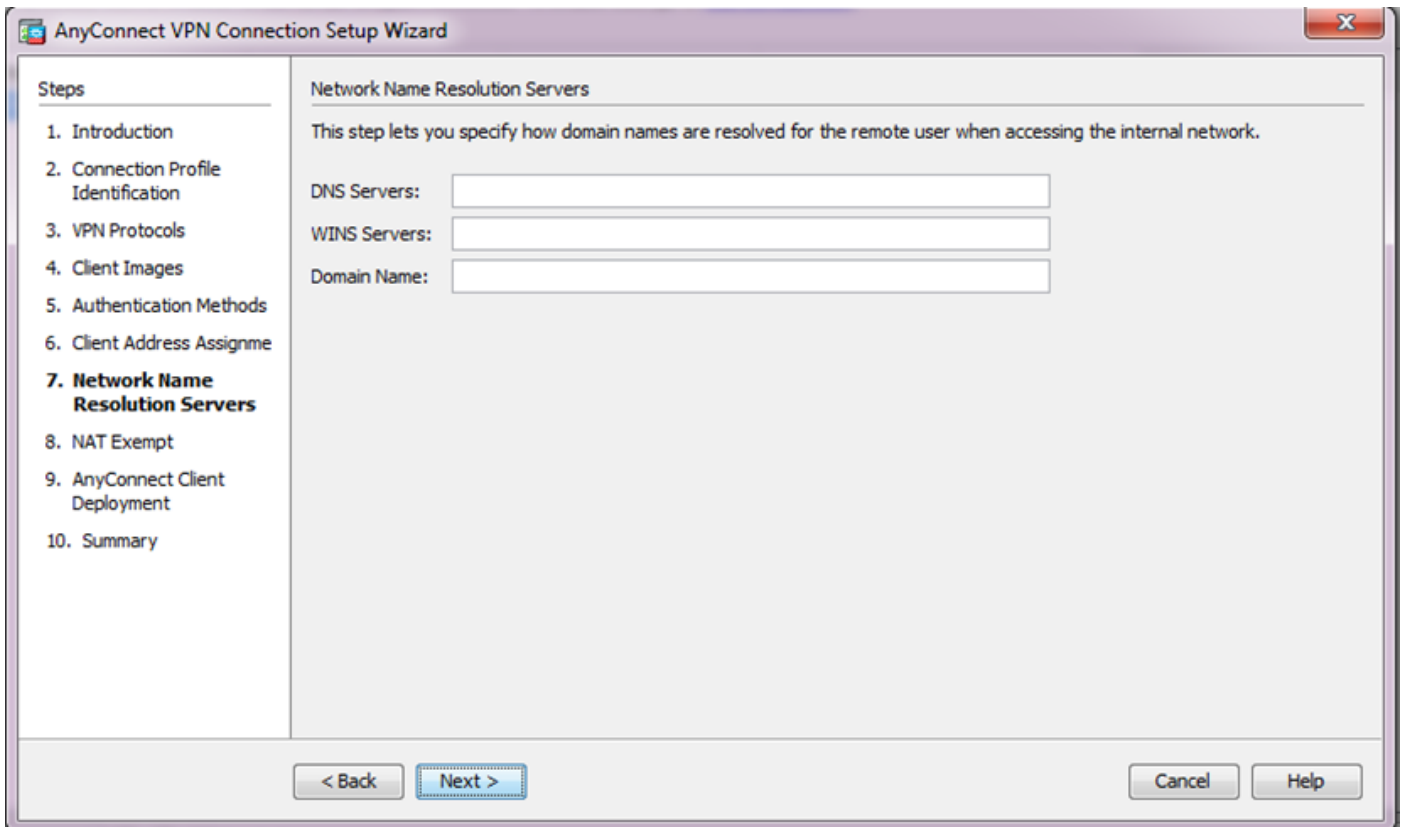




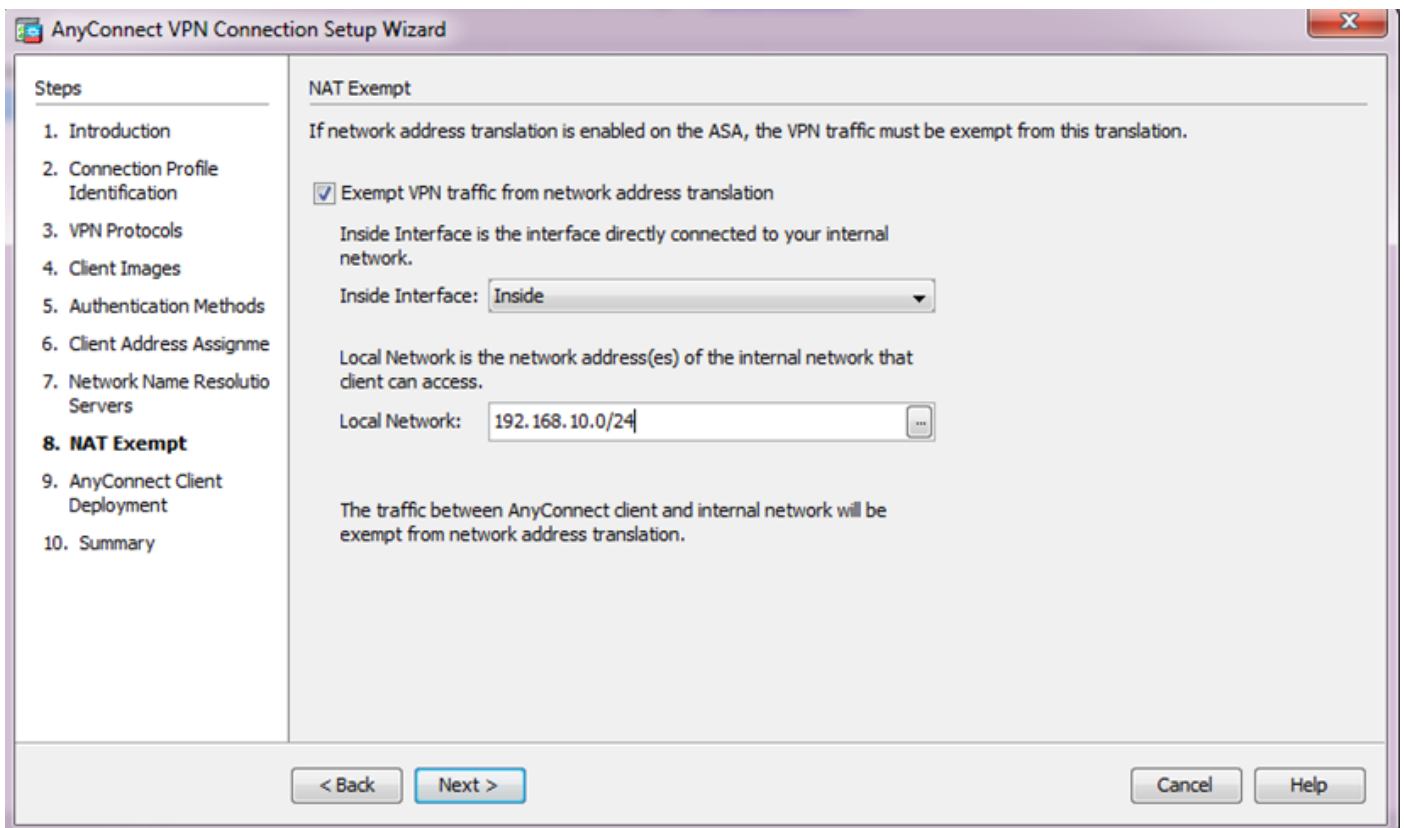
- 单击 Next。



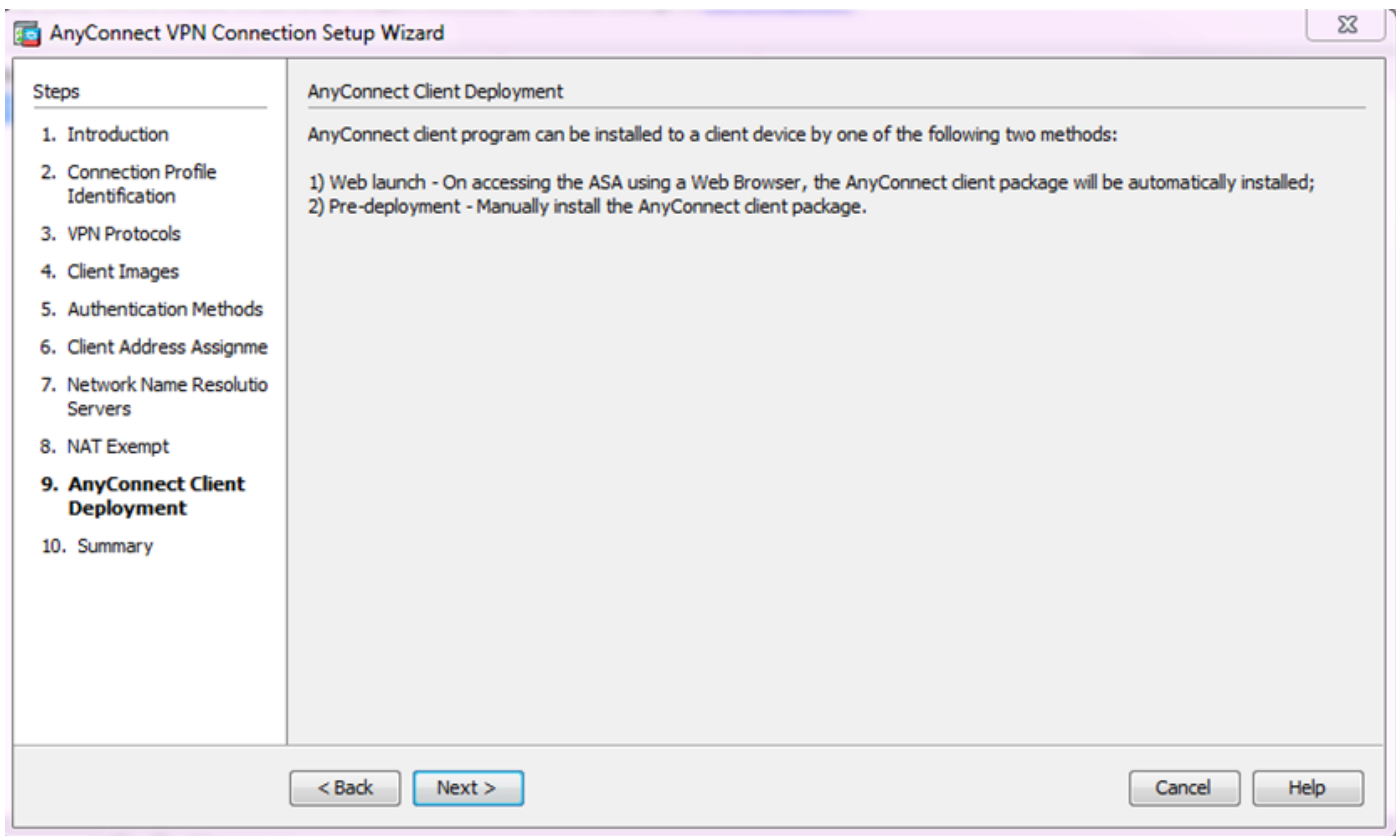
7. 随意地，请配置域名系统(DNS)服务器和Dns到DNS和域名字段，其次然后点击。



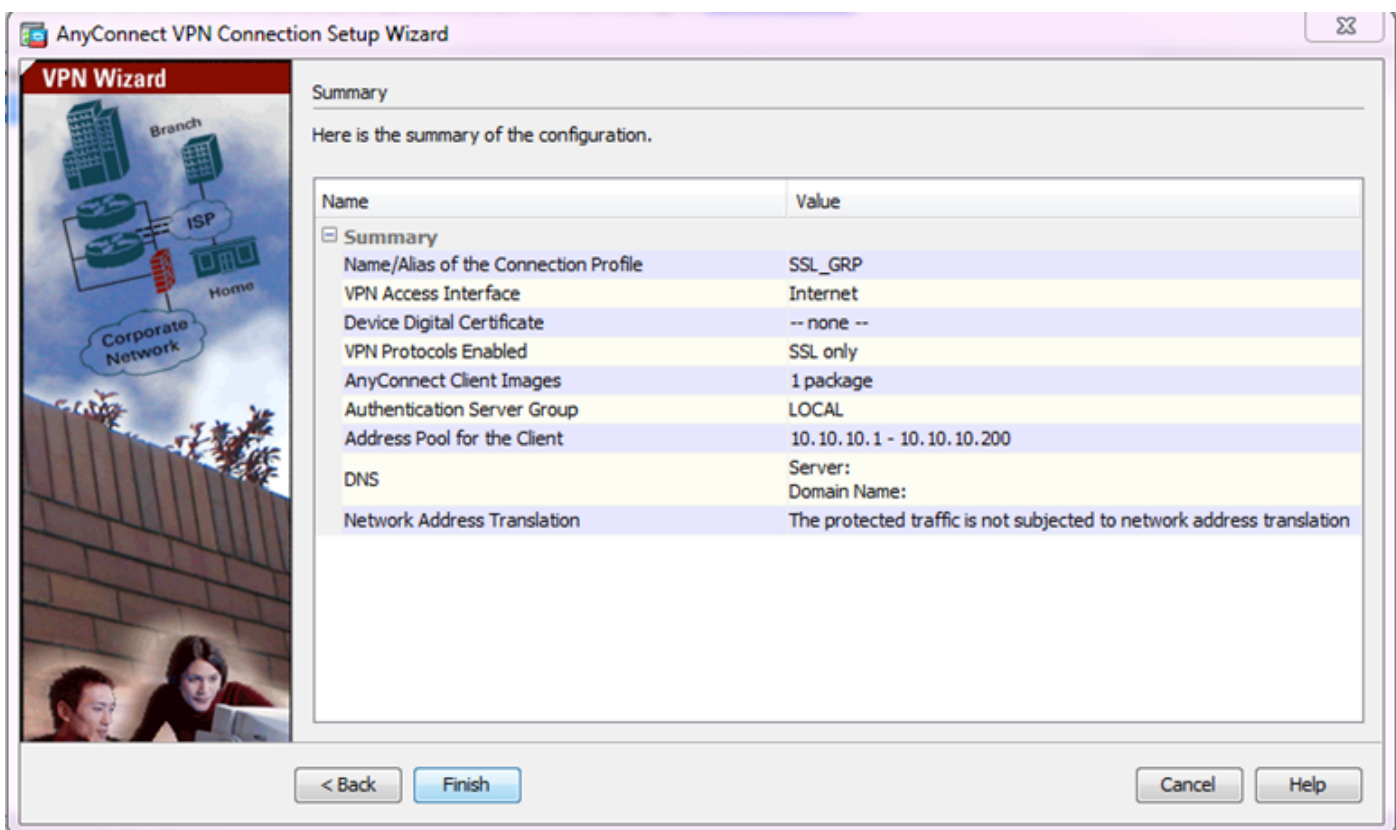
8. 保证客户端和内部的子网之间的数据流一定是豁免从所有动态网络地址转换(NAT)。Enable (event)从网络地址转换复选框的豁免VPN流量和配置将使用免税的LAN接口。并且，请指定必须豁免的本地网络并且其次点击。



9. 单击 Next。

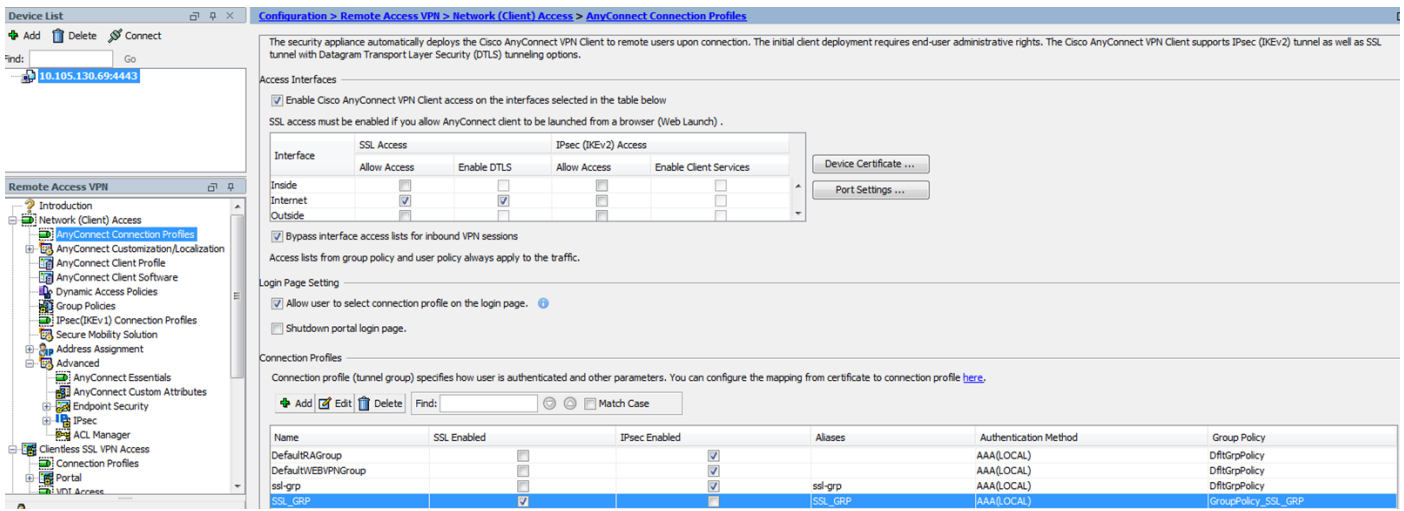


10. 最终步骤显示汇总，点击完成完成设置。

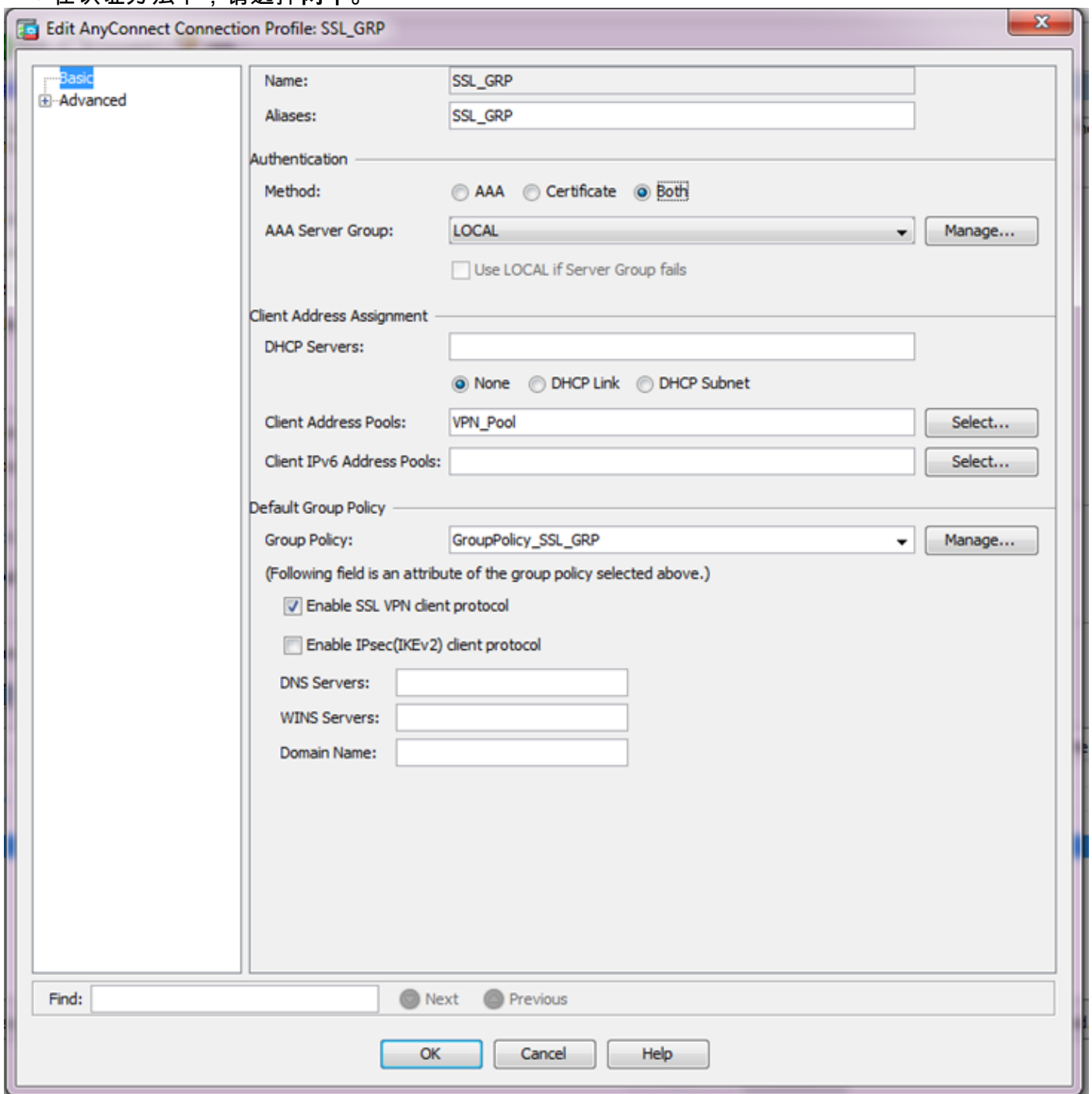


AnyConnect客户端配置当前完成。然而，当您通过配置向导时配置AnyConnect，默认情况下它配置认证方法作为AAA。为了通过证书和用户名/密码验证客户端，必须配置隧道组(连接配置文件)使用证书和AAA作为认证方法。

- 连接对Configuration>远程访问VPN >网络(客户端)访问> AnyConnect连接配置文件。
- 您应该看到SSL\_GRP列出的新的被添加的连接配置文件。



- 为了配置AAA和证书验证，选择连接配置文件SSL\_GRP和点击编辑。
- 在认证方法下，请选择两个。



## 配置AnyConnect的CLI

```
!! *****Configure the VPN Pool*****
```

```
ip local pool VPN_Pool 10.10.10.1-10.10.10.200 mask 255.255.255.0
```

```
!! *****Configure Address Objects for VPN Pool and Local Network*****
```

```
object network NETWORK_OBJ_10.10.10.0_24  
 subnet 10.10.10.0 255.255.255.0
```

```
object network NETWORK_OBJ_192.168.10.0_24 subnet 192.168.10.0 255.255.255.0 exit !!
```

```
*****Configure WebVPN*****
```

```
webvpn enable Internet anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1 anyconnect  
enable tunnel-group-list enable exit !! *****Configure User*****
```

```
username user1 password mbO2jYs13AXlIAGa encrypted privilege 2
```

```
!! *****Configure Group-Policy*****
```

```
group-policy GroupPolicy_SSL_GRP internal group-policy GroupPolicy_SSL_GRP attributes vpn-  
tunnel-protocol ssl-client dns-server none wins-server none default-domain none exit !!
```

```
*****Configure Tunnel-Group*****
```

```
tunnel-group SSL_GRP type remote-access  
tunnel-group SSL_GRP general-attributes  
 authentication-server-group LOCAL  
 default-group-policy GroupPolicy_SSL_GRP  
 address-pool VPN_Pool  
tunnel-group SSL_GRP webvpn-attributes  
 authentication aaa certificate  
 group-alias SSL_GRP enable  
 exit
```

```
!! *****Configure NAT-Exempt Policy*****
```

```
nat (Inside,Internet) 1 source static NETWORK_OBJ_192.168.10.0_24 NETWORK_OBJ_192.168.10.0_24  
destination static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24 no-proxy-arp route-lookup
```

## Verify

使用本部分可确认配置能否正常运行。

**Note:** [命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。使用输出解释器工具来查看 **show** 命令输出的分析。

保证CA服务器是启用的。

### 显示crypto加州服务器

```
ASA(config)# show crypto ca server  
Certificate Server LOCAL-CA-SERVER:  
  Status: enabled  
  State: enabled
```



Server's configuration is locked (enter "shutdown" to unlock it)

**Issuer name: CN=ASA.local**

CA certificate fingerprint/thumbprint: (MD5)  
32e868b9 351a1b07 4b59cce5 704d6615

CA certificate fingerprint/thumbprint: (SHA1)  
6136511b 14aa1bbe 334c2659 ae7015a9 170a7c4d

Last certificate issued serial number: 0x1

CA certificate expiration timer: 19:25:42 UTC Jan 8 2019

CRL NextUpdate timer: 01:25:42 UTC Jan 10 2016

Current primary storage dir: flash:/LOCAL-CA-SERVER/

Auto-Rollover configured, overlap period 30 days

Autorollover timer: 19:25:42 UTC Dec 9 2018

WARNING: Configuration has been modified and needs to be saved!!

保证用户允许登记在添加以后：

**\*\*\*\*\*Before Enrollment\*\*\*\*\***

ASA# **show crypto ca server user-db**

username: user1  
email: user1@cisco.com  
dn: CN=user1,OU=TAC  
allowed: 19:03:11 UTC Thu Jan 14 2016  
notified: 1 times  
enrollment status: Allowed to Enroll >>> **Shows the status "Allowed to Enroll"**

**\*\*\*\*\*After Enrollment\*\*\*\*\***

username: user1  
email: user1@cisco.com  
dn: CN=user1,OU=TAC  
allowed: 19:05:14 UTC Thu Jan 14 2016  
notified: 1 times  
**enrollment status: Enrolled**, Certificate valid until 19:18:30 UTC Tue Jan 10 2017,  
Renewal: Allowed

您可以通过CLI或ASDM检查anyconnect连接的详细资料。

## 通过CLI

### 显示vpn-sessiondb详细资料anyconnect

ASA# **show vpn-sessiondb detail anyconnect**

Session Type: AnyConnect Detailed

Username : user1 Index : 1  
Assigned IP : 10.10.10.1 Public IP : 10.142.189.181  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Essentials  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1  
Bytes Tx : 13822 Bytes Rx : 13299  
Pkts Tx : 10 Pkts Rx : 137  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : GroupPolicy\_SSL\_GRP Tunnel Group : SSL\_GRP  
Login Time : 19:19:10 UTC Mon Jan 11 2016  
Duration : 0h:00m:47s  
Inactivity : 0h:00m:00s

NAC Result : Unknown  
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1  
SSL-Tunnel Tunnels: 1  
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 1.1  
Public IP : 10.142.189.181  
Encryption : none Hashing : none  
TCP Src Port : 52442 TCP Dst Port : 443  
Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096  
Bytes Tx : 6911 Bytes Rx : 768  
Pkts Tx : 5 Pkts Rx : 1  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 1.2  
Assigned IP : 10.10.10.1 Public IP : 10.142.189.181  
Encryption : RC4 Hashing : SHA1  
Encapsulation: TLSv1.0 TCP Src Port : 52443  
TCP Dst Port : 443 Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096  
Bytes Tx : 6911 Bytes Rx : 152  
Pkts Tx : 5 Pkts Rx : 2  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 1.3  
Assigned IP : 10.10.10.1 Public IP : 10.142.189.181  
Encryption : AES128 Hashing : SHA1  
Encapsulation: DTLSv1.0 UDP Src Port : 59167  
UDP Dst Port : 443 Auth Mode : Certificate and userPassword  
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes  
Client OS : Windows  
Client Type : DTLS VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.2.00096  
Bytes Tx : 0 Bytes Rx : 12907  
Pkts Tx : 0 Pkts Rx : 142  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

NAC:

Reval Int (T): 0 Seconds Reval Left(T): 0 Seconds  
SQ Int (T) : 0 Seconds EoU Age(T) : 51 Seconds  
Hold Left (T): 0 Seconds Posture Token:  
Redirect URL :

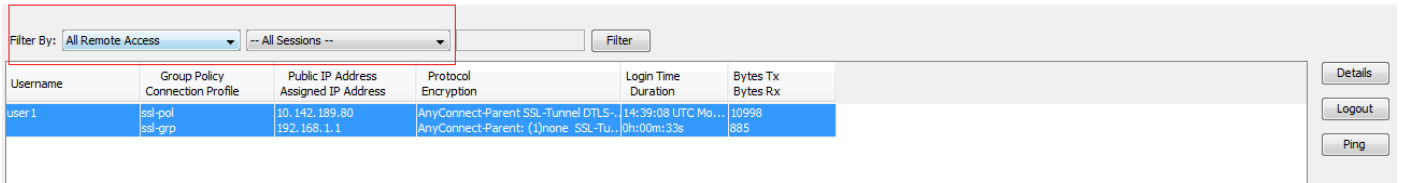
## 通过ASDM

- 连接对Monitoring> VPN > VPN统计数据>会话。
- 由作为所有远程访问选择过滤器。
- 您可以进行所选的AnyConnect客户端的动作之一。

详细资料提供关于会话的更多信息

退出手工退出从数据转发器的用户

连接从数据转发器连接AnyConnect客户端



The screenshot shows a web-based interface for monitoring sessions. At the top, there are filters for 'Filter By: All Remote Access' and '-- All Sessions --'. Below this is a table with columns: Username, Group Policy Connection Profile, Public IP Address, Assigned IP Address, Protocol Encryption, Login Time Duration, Bytes Tx, and Bytes Rx. The first row shows 'user 1' with group policy 'ssl-pol' and 'ssl-grp', public IP '10.142.189.80', assigned IP '192.168.1.1', protocol 'AnyConnect-Parent SSL-Tunnel DTLS...', login time '14:39:08 UTC Mo...', and bytes '10998 Tx, 885 Rx'. On the right side, there are buttons for 'Details', 'Logout', and 'Ping'.

Username	Group Policy Connection Profile	Public IP Address	Assigned IP Address	Protocol Encryption	Login Time Duration	Bytes Tx	Bytes Rx
user 1	ssl-pol ssl-grp	10.142.189.80	192.168.1.1	AnyConnect-Parent SSL-Tunnel DTLS...	14:39:08 UTC Mo...	10998	885

## Troubleshoot

本部分提供了可用于对配置进行故障排除的信息。

**Note:**使用 `debug` 命令之前，请参阅[有关 Debug 命令的重要信息](#)。

**警告：**在ASA，您能设置多种调试级别;默认情况下，使用第1级。如果更改调试级别，调试的冗余也许增加。执行此小心地，特别是在生产环境里。

- `debug crypto ca`
- `debug crypto ca`服务器
- `debug crypto ca`消息
- `debug crypto ca`处理
- 调试WebVPN anyconnect

当CA服务器使用`no shut`命令，是启用的此调试输出显示。

```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: input signal enqueued: no shut >>>> Command issued to Enable the CA server
Crypto CS thread wakes up!
```

```
CRYPTO_CS: enter FSM: input state disabled, input signal no shut
CRYPTO_CS: starting enabling checks
CRYPTO_CS: found existing serial file.
CRYPTO_CS: started CA cert timer, expiration time is 17:53:33 UTC Jan 13 2019
CRYPTO_CS: Using existing trustpoint 'LOCAL-CA-SERVER' and CA certificate
CRYPTO_CS: file opened: flash://LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: DB version 1
CRYPTO_CS: last issued serial number is 0x4
CRYPTO_CS: closed ser file
CRYPTO_CS: file opened: flash://LOCAL-CA-SERVER/LOCAL-CA-SERVER.crl
CRYPTO_CS: CRL file LOCAL-CA-SERVER.crl exists.
CRYPTO_CS: Read 220 bytes from crl file.
CRYPTO_CS: closed crl file
CRYPTO_PKI: Storage context locked by thread Crypto CA Server
```

```
CRYPTO_PKI: inserting CRL
CRYPTO_PKI: set CRL update timer with delay: 20250
CRYPTO_PKI: the current device time: 18:05:17 UTC Jan 16 2016
```

```
CRYPTO_PKI: the last CRL update time: 17:42:47 UTC Jan 16 2016
CRYPTO_PKI: the next CRL update time: 23:42:47 UTC Jan 16 2016
CRYPTO_PKI: CRL cache delay being set to: 20250000
CRYPTO_PKI: Storage context released by thread Crypto CA Server
```

```
CRYPTO_CS: Inserted Local CA CRL into cache!
```

```
CRYPTO_CS: shadow not configured; look for shadow cert
CRYPTO_CS: failed to find shadow cert in the db
CRYPTO_CS: set shadow generation timer
CRYPTO_CS: shadow generation timer has been set
CRYPTO_CS: Enabled CS.
CRYPTO_CS: exit FSM: new state enabled
CRYPTO_CS: cs config has been locked.
```

```
Crypto CS thread sleeps!
```

## 此调试输出显示客户端的登记

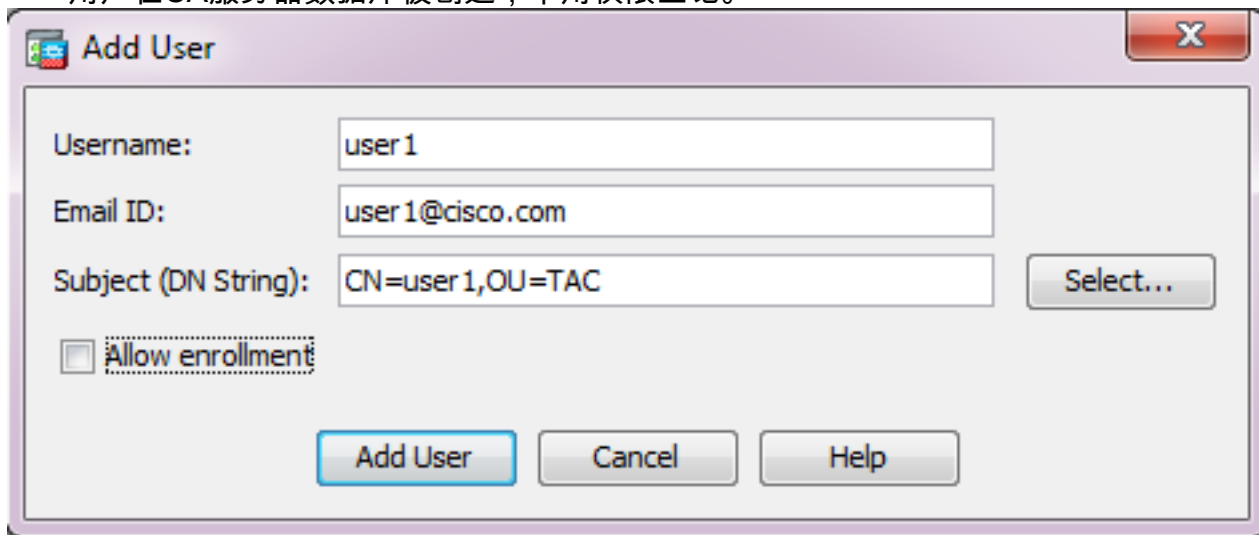
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12
```

## 客户端的登记可能失效在这些conditons下：

### 方案1。

- 用户在CA服务器数据库被创建，不用权限登记。

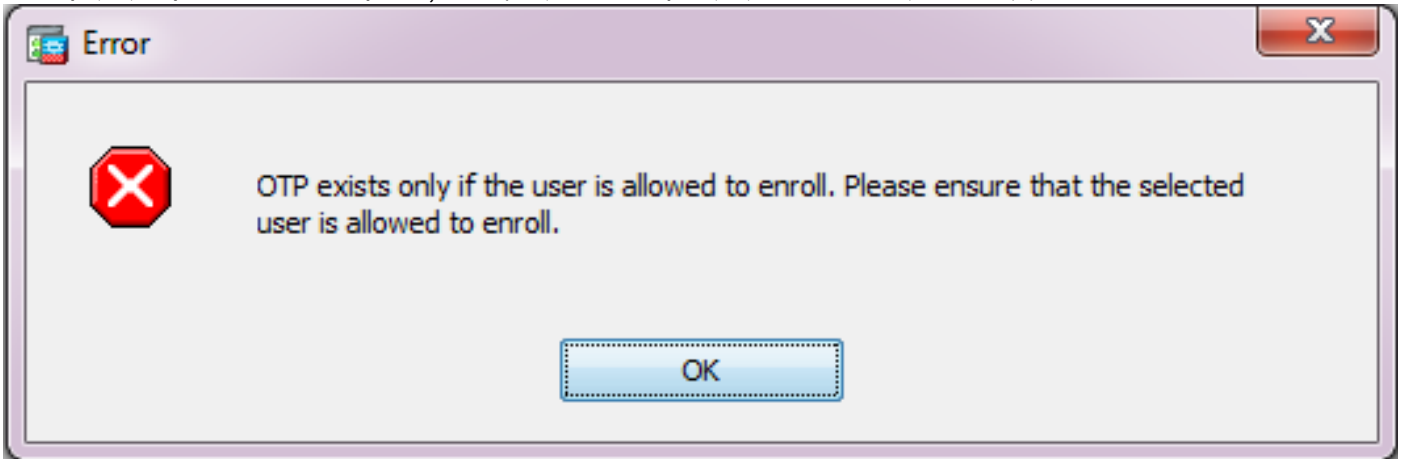


## 等效的 CLI 命令：

```
ASA(config)# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:      CN=user1,OU=TAC
```

```
allowed: <not allowed>
notified: 0 times
enrollment status: Not Allowed to Enroll
```

- 在用户不允许登记的事件，尝试生成/电子邮件用户的OTP生成此错误信息。



## 场景 2：

- 验证端口并且建立接口在哪些登记门户是可用的使用webvpn命令的show run。默认端口是443，但是可以被修改。
- 保证客户端有网络可达性对WebVPN在用于的端口被启用顺利地访问登记门户接口的IP地址。客户端可能不能在这些情况下访问ASA登记门户：
  1. 如果任何中间设备阻拦从客户端的流入的连接与ASA的WebVPN IP在端口的指定的。
  2. 接口的状态下降在哪WebVPN是启用的。
- 此输出表示，登记门户是可用的在接口互联网的IP地址自定义端口的4433。

```
ASA(config)# show run webvpn
webvpn
port 4433
enable Internet
no anyconnect-essentials
anyconnect image disk0:/anyconnect-win-4.2.00096-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

## 场景 3：

- CA服务器数据库存储的默认位置是ASA的闪存。
- 保证闪存有空闲空间生成和保存用户的pkcs12文件在登记期间。
- 在闪存没有足够的空闲空间的案件，ASA不能完成客户端的登记进程并且生成这些调试日志：

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash://LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
```

CRYPTO\_CS: Generated and saving a PKCS12 file for user user1  
at flash:/LOCAL-CA-SERVER/user1.p12

CRYPTO\_CS: Failed to write to opened PKCS12 file for user user1, fd: 0, status: -1.

CRYPTO\_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO\_CS: Failed to process enrollment in-line for user user1. status: -1

## Related Information

- [Cisco ASA 5500 系列自适应安全设备](#)
- [AnyConnect VPN 客户端故障排除指南 - 常见问题](#)
- [管理，监控和排除AnyConnect会话故障](#)
- [Technical Support & Documentation - Cisco Systems](#)