

Configurar o ASA como um server CA e um final do cabeçalho locais de AnyConnect

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[ASA como um server local CA](#)

[Etapa 1. Configurar e permita o server local CA no ASA](#)

[Etapa 2. Crie e adicionar usuários ao base de dados ASA](#)

[Etapa 3. Permita o webvpn na interface WAN](#)

[Etapa 4. Importe o certificado na máquina cliente](#)

[ASA como um gateway SSL para clientes de AnyConnect](#)

[Wizard de configuração ASDM AnyConnect](#)

[Configurar o CLI para AnyConnect](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este original descreve como setup uma ferramenta de segurança adaptável de Cisco (ASA) como um server do Certificate Authority (CA) e como um gateway do secure sockets layer (SSL) para Clientes de mobilidade Cisco AnyConnect Secure.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração básica ASA que executa a versão de software 9.1.x
- ASDM 7.3 ou mais alto

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 5500 Series ASA que executa a versão de software 9.1(6)

- Versão de cliente segura 4.x da mobilidade de AnyConnect para Windows
- PC que executa um ósmio apoiado pela [carta da compatibilidade](#).
- Versão 7.3 do Cisco Adaptive Security Device Manager (ASDM)

Nota: Faça download do pacote do AnyConnect VPN Client (anyconnect-win*.pkg) do [Download de Software Cisco \(somente clientes registrados\)](#). Copie o AnyConnect VPN client para a memória flash do ASA, a qual será transferida para os computadores do usuário remoto a fim de estabelecer a conexão VPN SSL com o ASA. Consulte a seção [Instalação do AnyConnect Client](#) do guia de configuração do ASA para obter mais informações.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O Certificate Authority no ASA fornece estas funcionalidades:

- Integra a operação básica do Certificate Authority no ASA.
- Distribui Certificados.
- Fornece a verificação segura da revogação de Certificados emitidos.
- Fornece um Certificate Authority no ASA para o uso as conexões de VPN do navegador-based(WebVPN) e do cliente-based(AnyConnect) SSL.
- Certificados digitais confiados Provides aos usuários, sem a necessidade de confiar na autorização externo do certificado.
- Fornece uma autoridade segura, da em-casa para o certificado de autenticação e um registro direto do usuário das ofertas por meio de um início de uma sessão do Web site.

Diretrizes e limitações

- Apoiado no modo de firewall roteado e transparente.
- Somente um server local CA de cada vez pode ser residente em um ASA.
- O ASA como uma característica local do server CA não é apoiado em uma instalação do Failover.
- O ASA a partir de agora que atua como um server local CA apoia somente a geração dos Certificados SHA1.
- O server local CA pode ser usado para conexões de VPN com base em navegador e cliente-baseadas SSL. Atualmente não apoiado para IPSec.
- Não apoia o Balanceamento de carga VPN para o CA local.
- O CA local não pode ser um subordinado a um outro CA. Pode atuar somente como a CA raiz.
- Atualmente o ASA não pode registrar-se ao server local CA para o certificado de identidade.
- Quando um certificado de registro é terminado, o ASA armazena um arquivo do PKCS12 que contém o keypair e o certificate chain do usuário, que exige aproximadamente 2 KB da memória Flash ou do espaço de disco pelo registro. A quantidade real do espaço de disco depende dos campos configurados do tamanho chave e do certificado RSA. Mantenha esta diretriz na mente ao adicionar um grande número certificados de registro pendentes em um

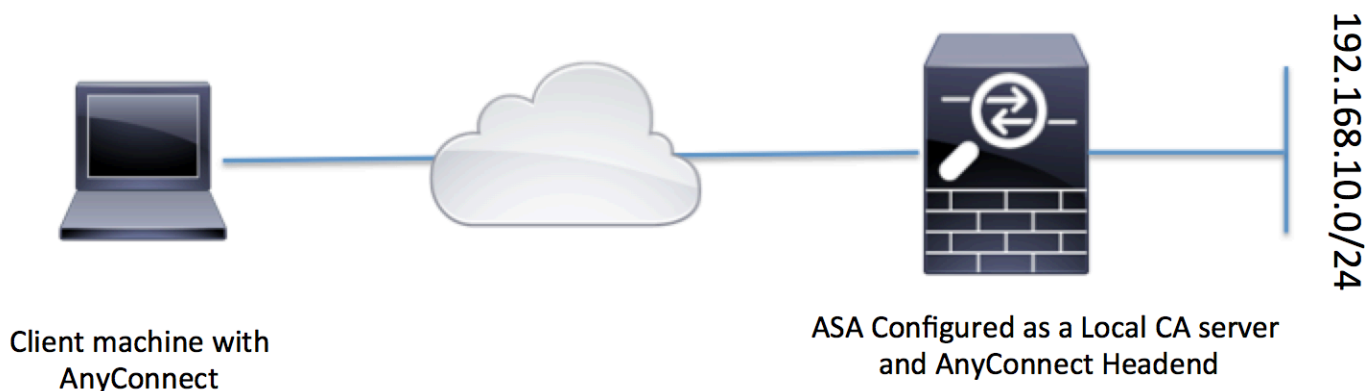
ASA com uma quantidade limitada de memória Flash disponível, porque estes arquivos do PKCS12 são armazenados na memória Flash para a duração do intervalo configurado da recuperação do registro.

Configurar

Esta seção descreve como configurar Cisco ASA como um server local CA.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede



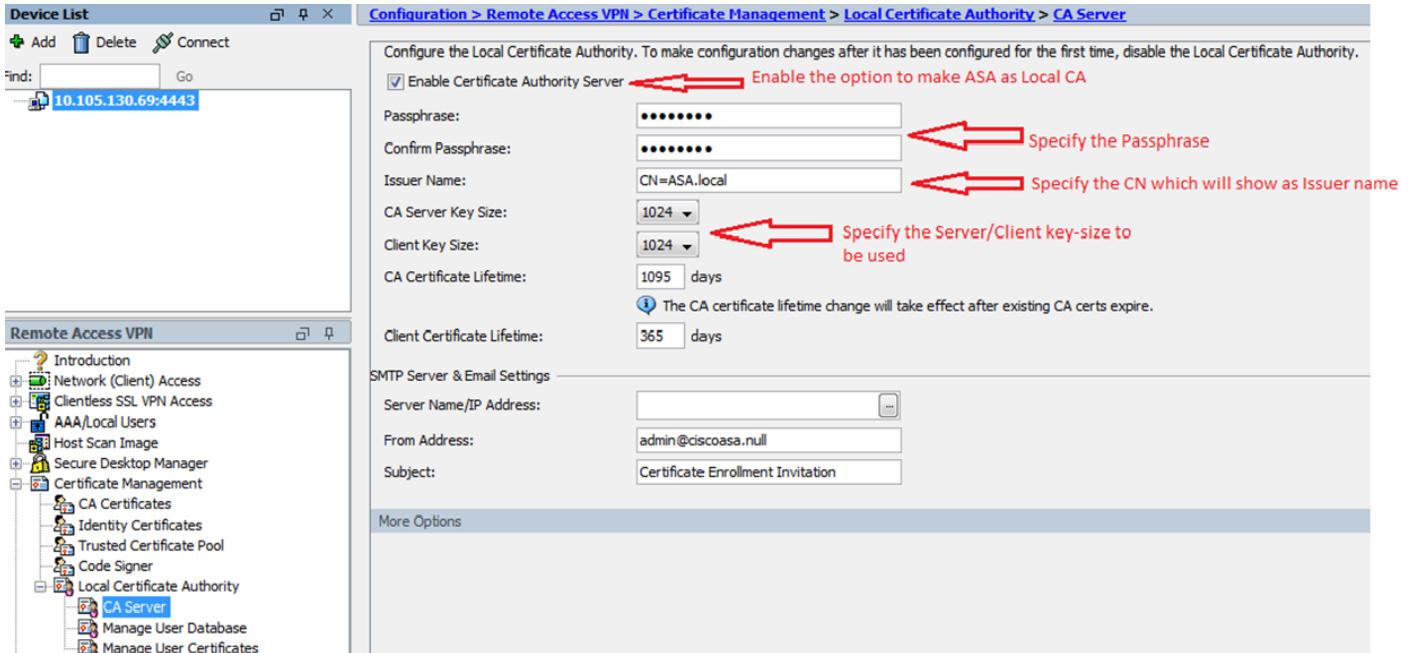
ASA como um server local CA

Etapa 1. Configurar e permita o server local CA no ASA

- Navegue à **configuração > ao acesso remoto VPN > ao gerenciamento certificado > Certificate Authority local > server CA**. Verifique a **opção Server do Certificate Authority da possibilidade**.
- Configurar a frase de passagem. A frase de passagem deve ser um mínimo, os caracteres 7 que seja usado para codificar e salvar um arquivo do PKCS12 que inclua o certificado de CA e o par de chaves locais. A frase de passagem destrava o arquivo do PKCS12 se o certificado de CA ou o keypair são perdidos.
- Configurar o nome de emissor. Este campo apareceria como a NC do certificado de raiz. Isto pode ser especificado no seguinte formato: NC (Common Name), OU (unidade da organização), (O) organização, L (localidade), S (estado) e C (país).
- **Configuração opcional:** Configurar o servidor SMTP e as configurações de servidor do email para assegurar o OTP poderiam ser recebidas para terminar clientes através do correio para terminar o registro. Você pode configurar o hostname ou o IP address de seu server local

Email/SMTP. Você pode igualmente configurar do **endereço** e do **campo de assunto** do email que os clientes receberiam. À revelia, do endereço é o **admin@<ASA hostname>.null** e o **assunto é convite do certificado de registro.**

- **Configuração opcional:** Você pode configurar os parâmetros opcionais como o **tamanho do tamanho chave do cliente, da chave de servidor CA, a vida da vida do certificado Ca e do certificado de cliente também.**



Equivalente CLI:

```
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

Estes são os campos adicionais que poderiam ser configurados sob a configuração do servidor local CA.

CRL	Este é o lugar CRL no ASA.
Distribution Point URL	O local padrão é http://hostname.domain/+CSCOCA+/asa_ca.crl mas a URL poderia ser alterada.
Relação Publicar-CRL e porta	Para fazer o CRL disponível para a transferência HTTP em uma dada interface e em uma porta, escolha uma relação publicar-CRL da lista de drop-down. Entre então no número de porta, que pode ser qualquer número de porta de 1-65535. O número de porta padrão é a porta TCP 80.
Tempo vida de CRL	As atualizações locais CA e reeditam o CRL cada vez que um certificado de usuário é revogado ou unrevoked, mas se há nenhuma revogação muda, o CRL é reeditada automaticamente uma vez que cada tempo vida de CRL, o período de tempo onde

Se você especifica com o **crllcommand da vida** durante a configuração local CA. Se você não especifica um tempo vida de CRL, o período de tempo padrão é **seis horas**.

Local de armazenamento do base de dados A informação de usuário dos acessos e dos implementares ASA, Certificados emitidos, e listas de revogação usando um base de dados local CA. **Este base de dados reside na memória Flash local à revelia**, ou pode ser configurado para residir em um sistema de arquivos externo que seja montado e acessível ao ASA.

Incorpore um assunto do padrão (corda DN) para adicionar a um username em Certificados emitidos. Os atributos permitidos DN são fornecidos nesta lista:

- NC (Common Name) SN (sobrenome)
- O (nome de organização)
- L (localidade)
- C (país)
- OU (unidade da organização)
- EA (endereço email)
- ST (estado/província)
- T (título)

Nome do sujeito do padrão Ajusta o limite de tempo do registro nas horas dentro de que o usuário poderia recuperar o arquivo do PKCS12 do ASA.

Período de registro O valor padrão é 24 horas.

Nota: Se o período de registro expira antes que o usuário recupere o arquivo do PKCS12 que inclui o certificado de usuário, o registro não é permitido.

Uma expiração de senha do tempo Define a quantidade de tempo nas horas que o OTP é válido para o registro do usuário. Este período de tempo começa quando é permitido ao usuário se registrar. O valor do default é 72 horas.

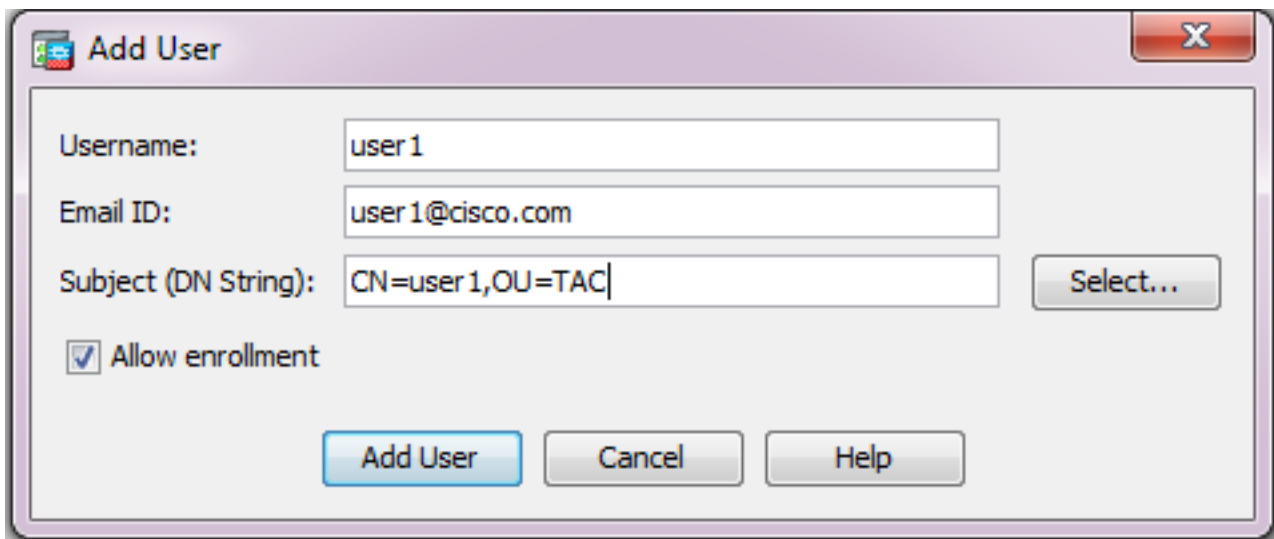
Lembrete da expiração do certificado Especifica o número de dias antes que o certificado expire que um lembrete inicial ao reenroll está enviado para certificate proprietários.

Etapa 2. Crie e adicionar usuários ao base de dados ASA

- Navegue à **configuração > ao acesso remoto VPN > ao gerenciamento certificado > Certificate Authority local > controlam o usuário que Database.** Click adicionam.



- Especifique o usuário detalha a saber a identificação username, de email e o nome do sujeito, segundo as indicações desta imagem.

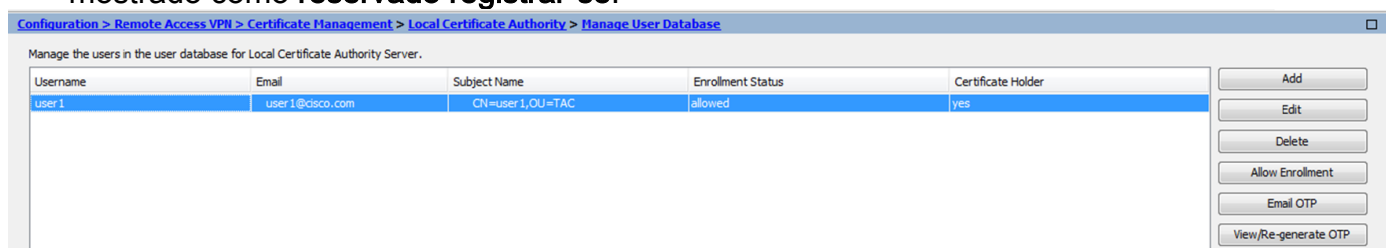


- Assegure-se de que que **reserva o registro** é verificado de modo que seja permitido você se registrar para o certificado.
- O clique **adiciona o usuário** para terminar a configuração do usuário.

Equivalente CLI:

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

- Depois que o usuário é adicionado à base de dados de usuário, o estado do registro está mostrado como **reservado registrar-se**.



CLI para verificar o estado do usuário:

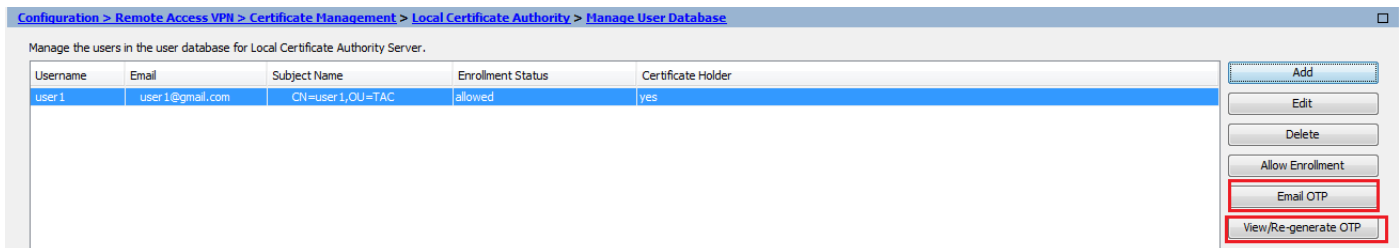
```
ASA# show crypto ca server user-db
```

```
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
```

- Depois que o usuário foi adicionado à base de dados de usuário, a uma senha do tempo (OTP), para que o usuário termine o registro, pode ser fornecida usando qualquer um isto: Envie por correio eletrônico o OTP (exige o servidor SMTP e enviam por correio eletrônico os ajustes a ser configurados sob a configuração do servidor CA).

OU

Veja diretamente o OTP e a parte com o usuário clicando em View/Re-generate OTP. Isto pode igualmente ser usado ao regenrate o OTP.



Equivalente 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
```

Etapa 3. Permita o webvpn na interface WAN

- Permita o acesso à Web no ASA para que os clientes peçam para o registro.

```
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
```

Etapa 4. Importe o certificado na máquina cliente

- Na estação de trabalho cliente abra um navegador e navegue à relação a fim terminar o registro.
- O IP/FQDN usado nesta relação deve ser o IP da relação em que o **webvpn** é permitido nessa etapa, que é **Internet da relação**.

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

- Incorpore o username (configurado no ASA sob etapa 2, a opção A) e o **OTP**, que foi fornecido através do **email** ou **manualmente**.

Browser window showing the ASA - Local Certificate Authority login page. The URL is <https://10.105.130.69/+CSCOCA+/login.html>. The page title is "ASA - Local Certificate Authority".

The login form contains the following fields and buttons:

- Username: user1
- One-time Password: [Redacted]
- Submit button
- Reset button

A red arrow points to the One-time Password field with the text: "Enter the User-Name and OTP provided".


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

- Clique **aberto** para instalar diretamente o certificado de cliente recebido do ASA.
- A frase de passagem para instalar o certificado de cliente é mesma como o OTP recebeu mais cedo.

File Download dialog box titled "File Download".

Do you want to open or save this file?

 Name: user1.p12
Type: Personal Information Exchange
From: 10.105.130.214

Buttons: Open, Save, Cancel

Warning message: 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?](#)

- Clique em Next.



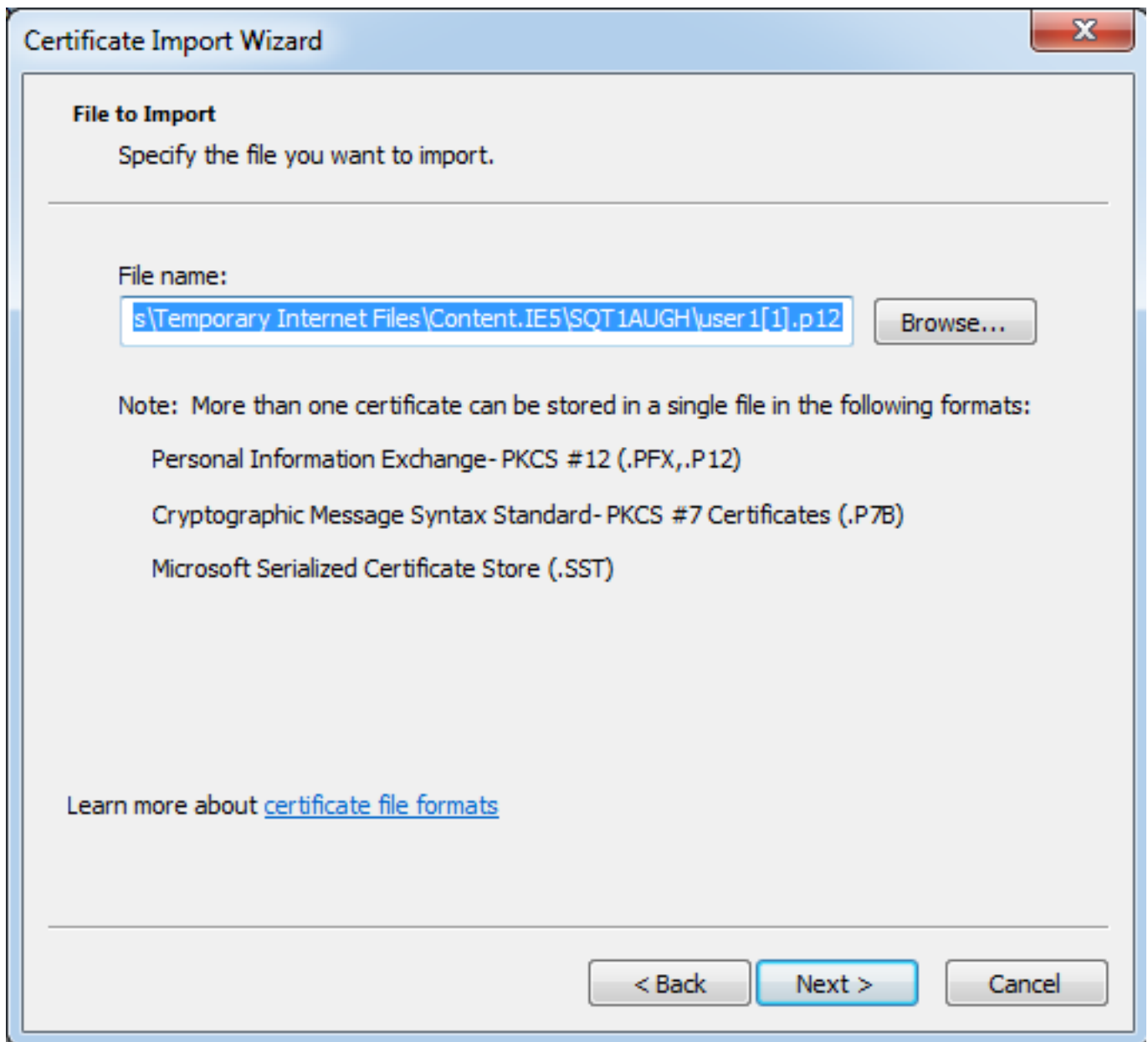
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

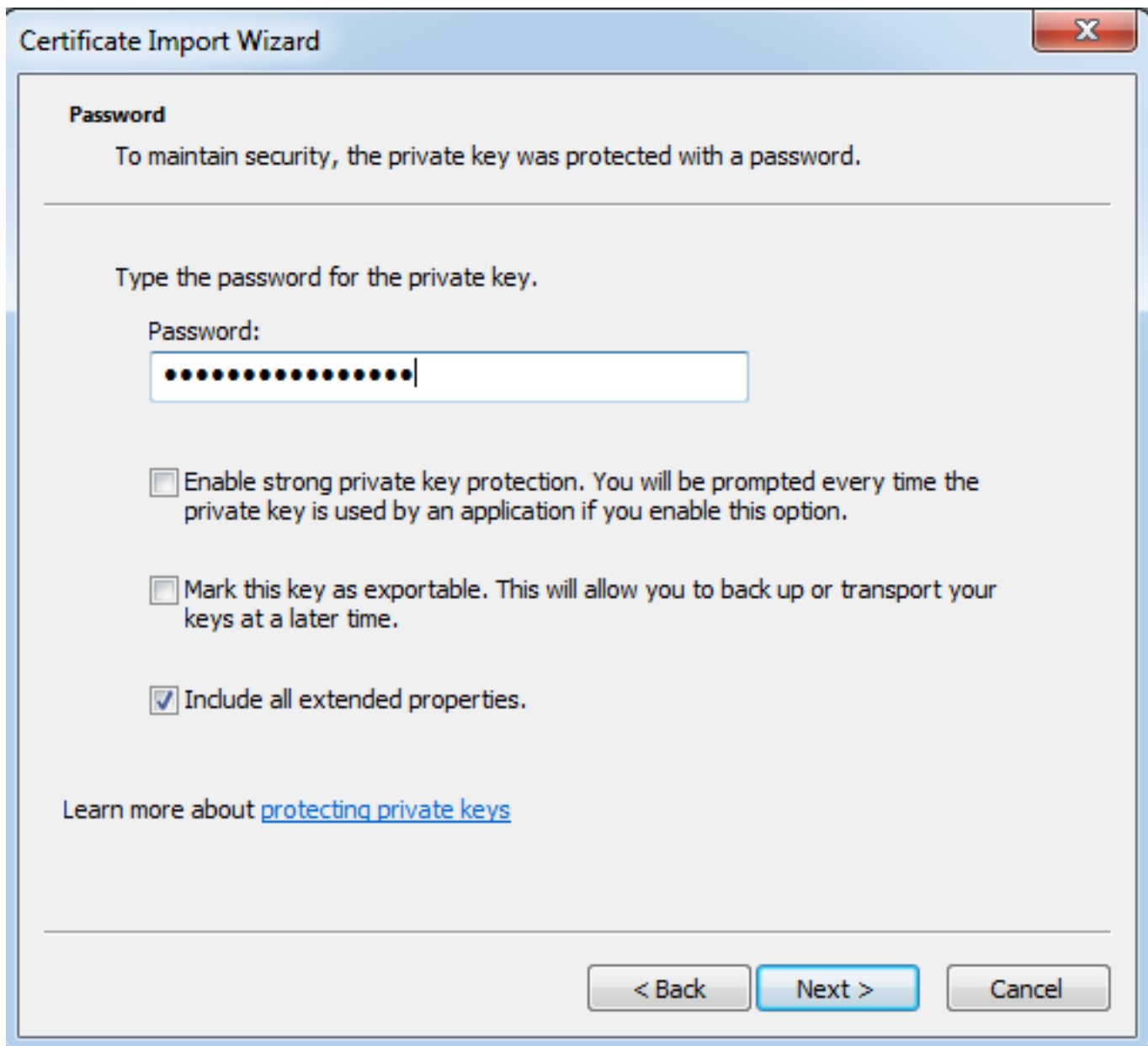
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

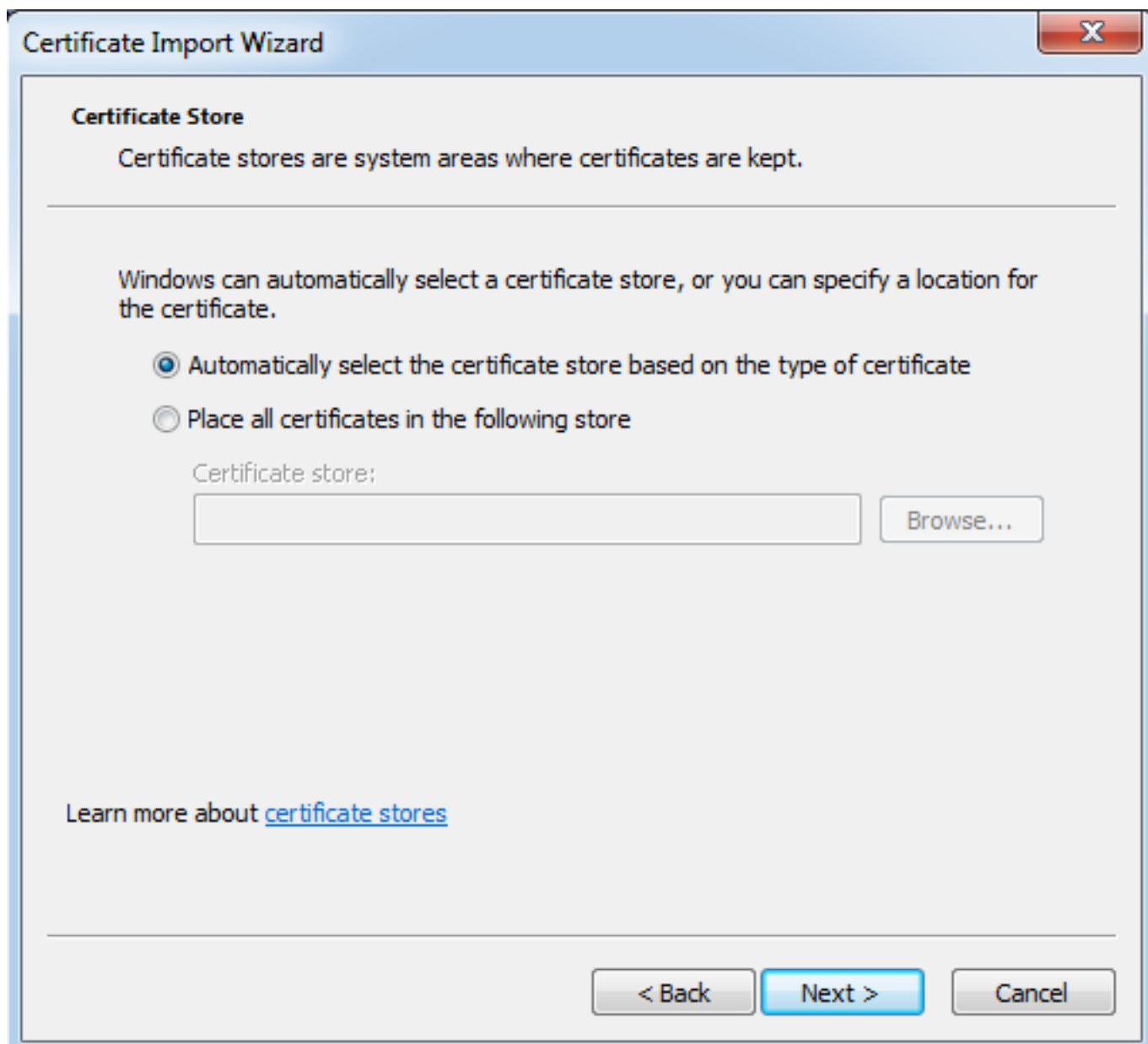
- Deixe o trajeto como o padrão e clique-o em seguida.



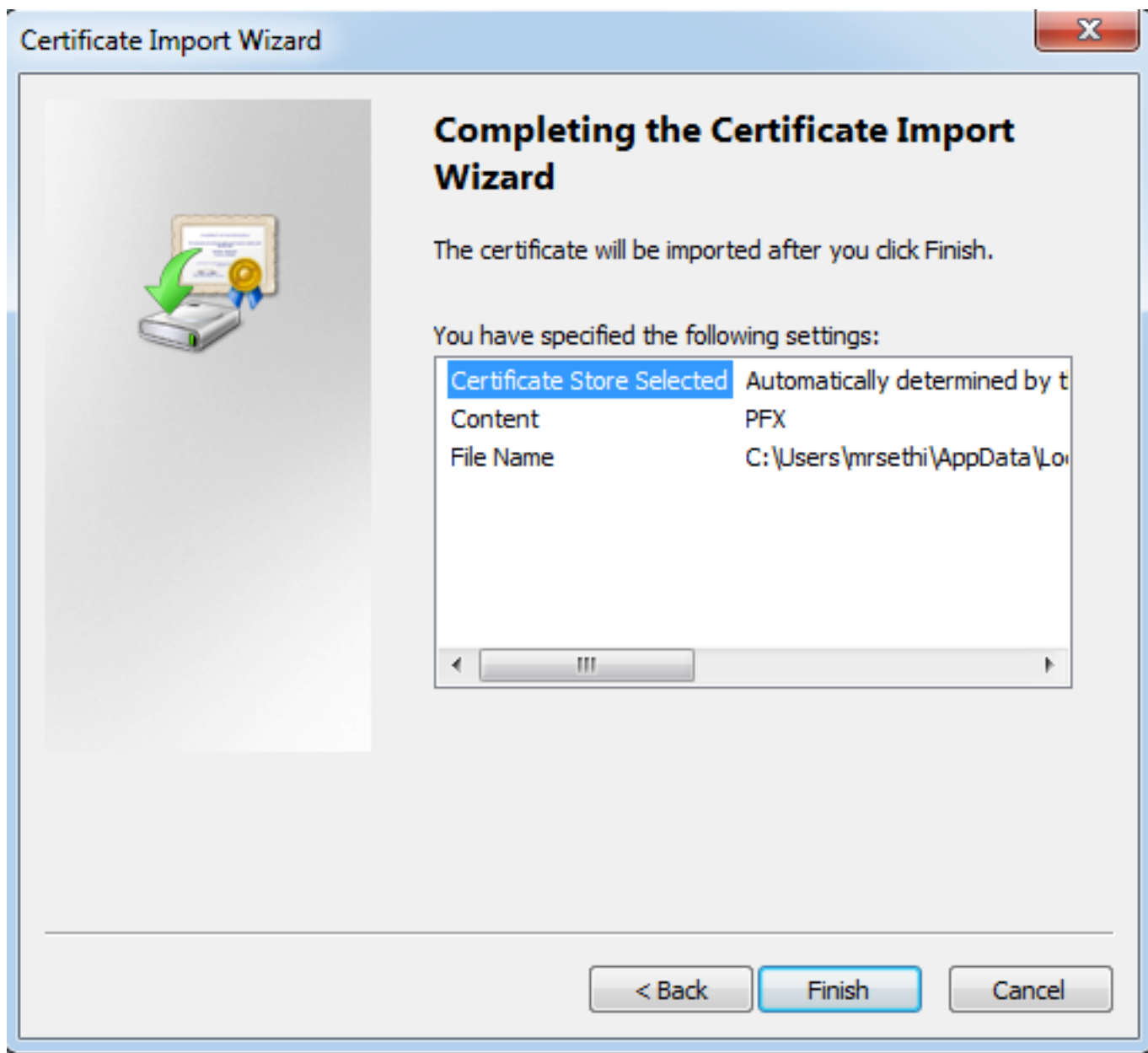
- Incorpore o OTP ao campo de senha.
- Você pode selecionar a opção **para marcar esta chave como exportable** de modo que a chave pudesse ser exportada da estação de trabalho no futuro se for necessário.
- Clique **em seguida**



- Você pode manualmente instalar o certificado em uma loja particular do certificado ou deixá-lo para escolher automaticamente a loja.
- Clique em Next.

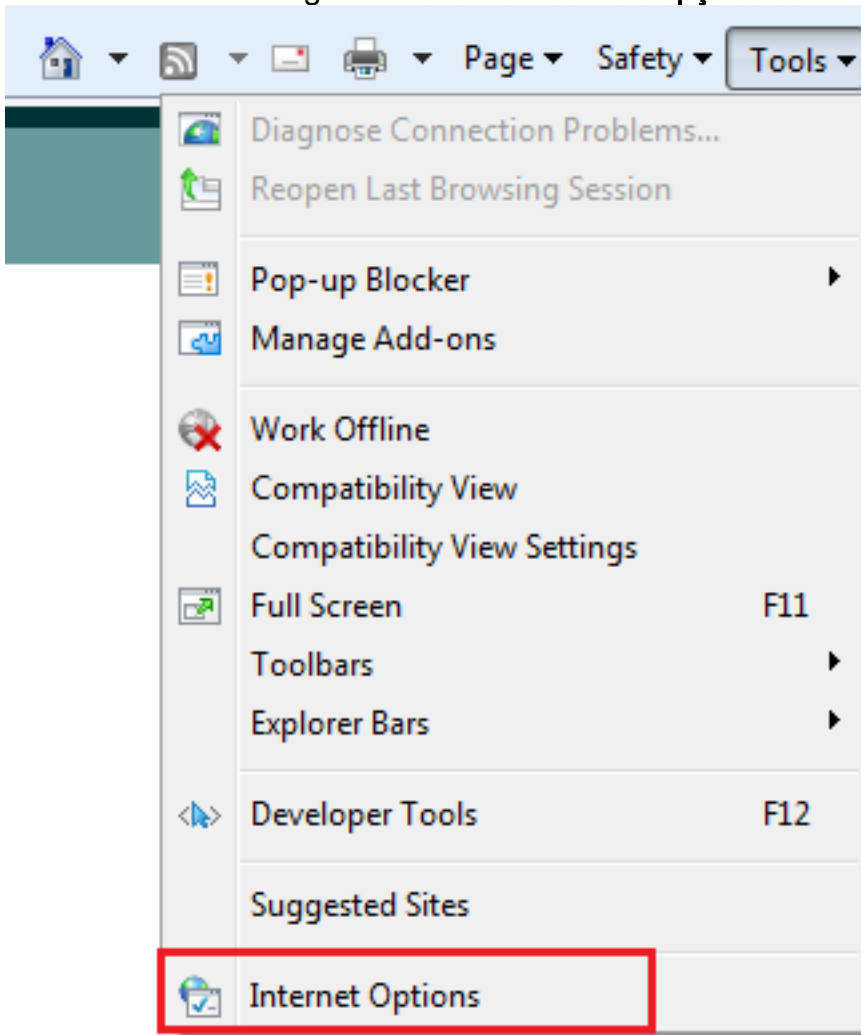


- **Revestimento do clique** a fim terminar a instalação.

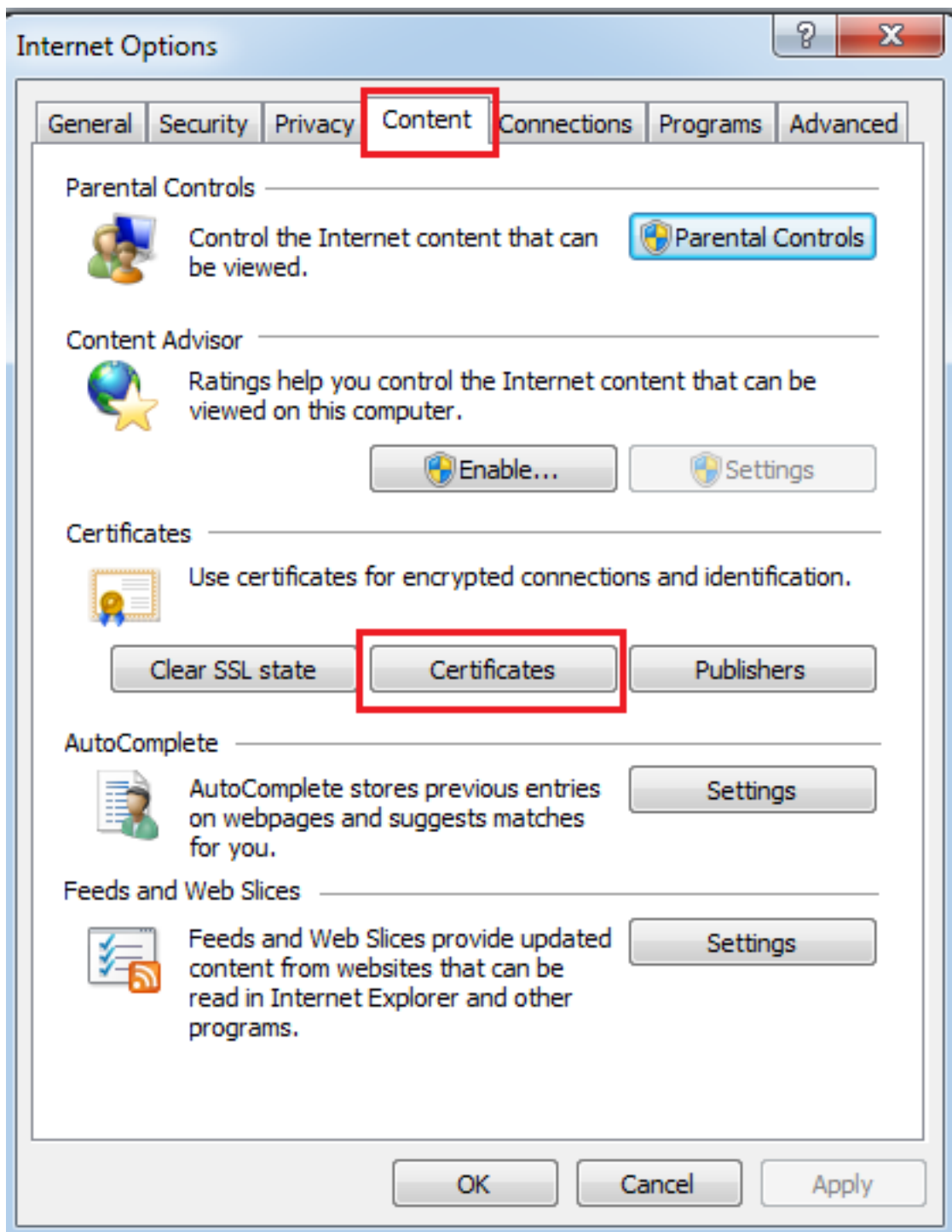


- Uma vez que o certificado é instalado com sucesso, você pode verificá-lo.

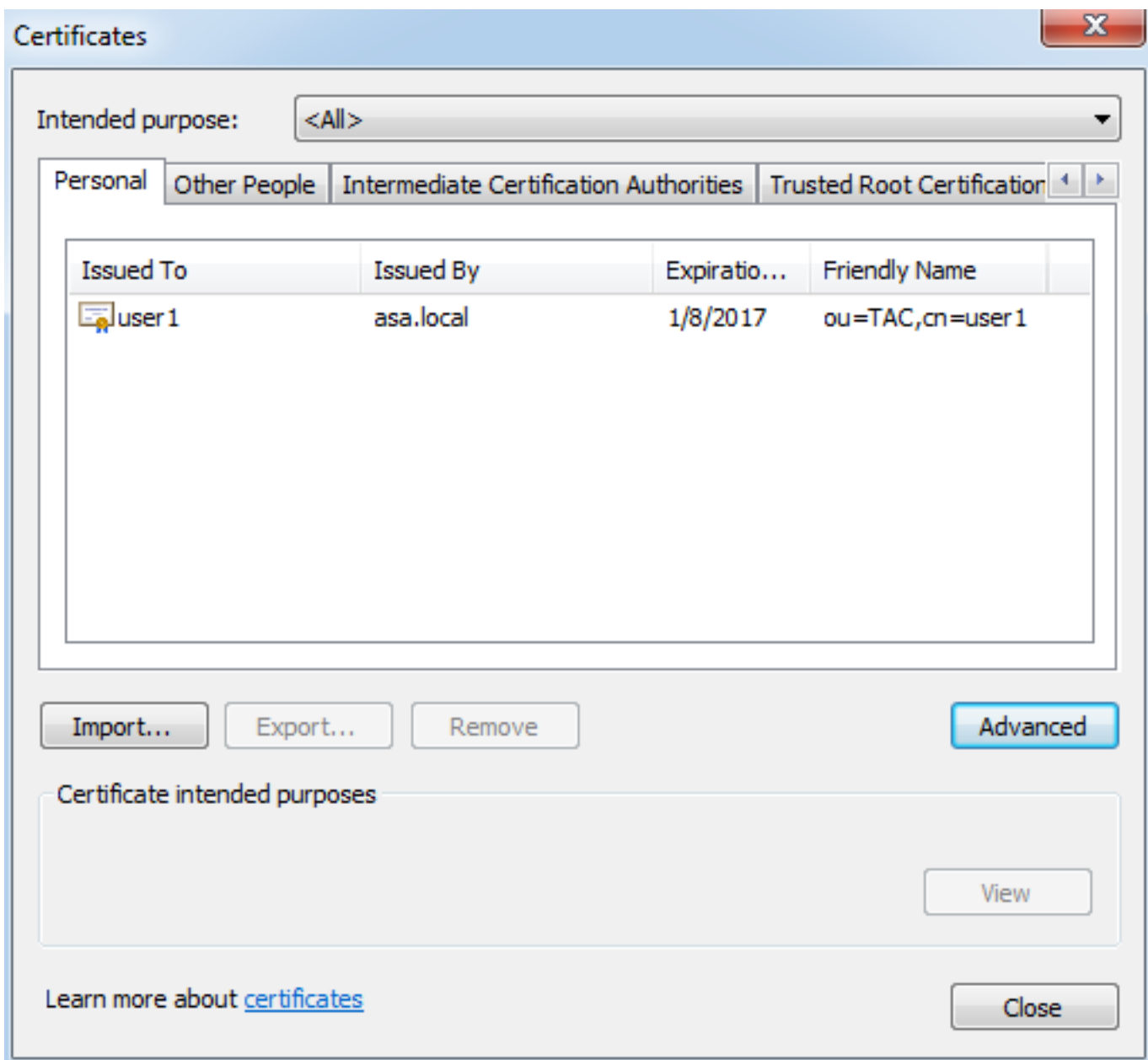
- Abra o IE e navegue às **ferramentas > às opções de internet**.



- Navegue **para satisfazer a aba** e clicar **Certificados**, segundo as indicações desta imagem.



- Sob a loja pessoal, você pode ver o certificado recebido do ASA.



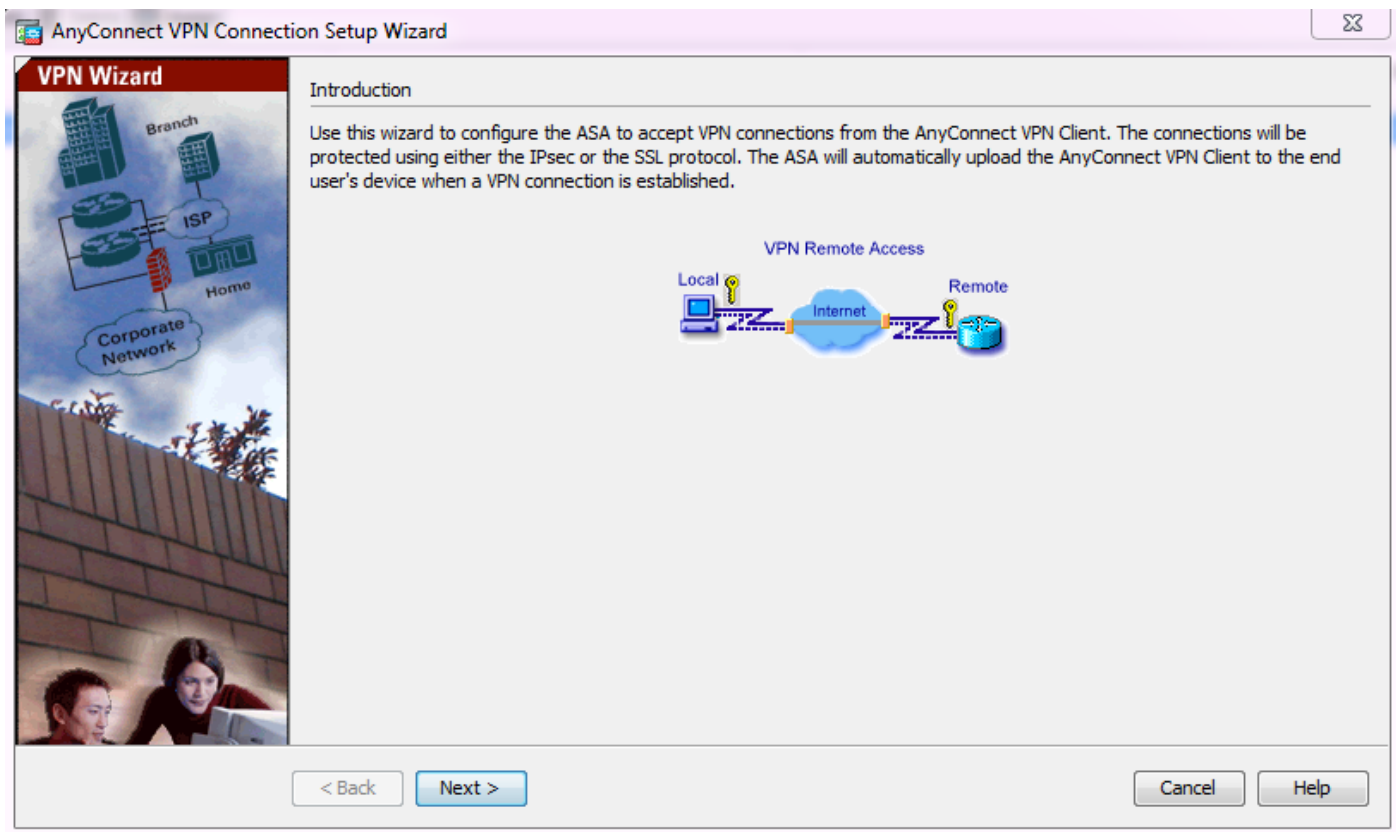
ASA como um gateway SSL para clientes de AnyConnect

Wizard de configuração ASDM AnyConnect

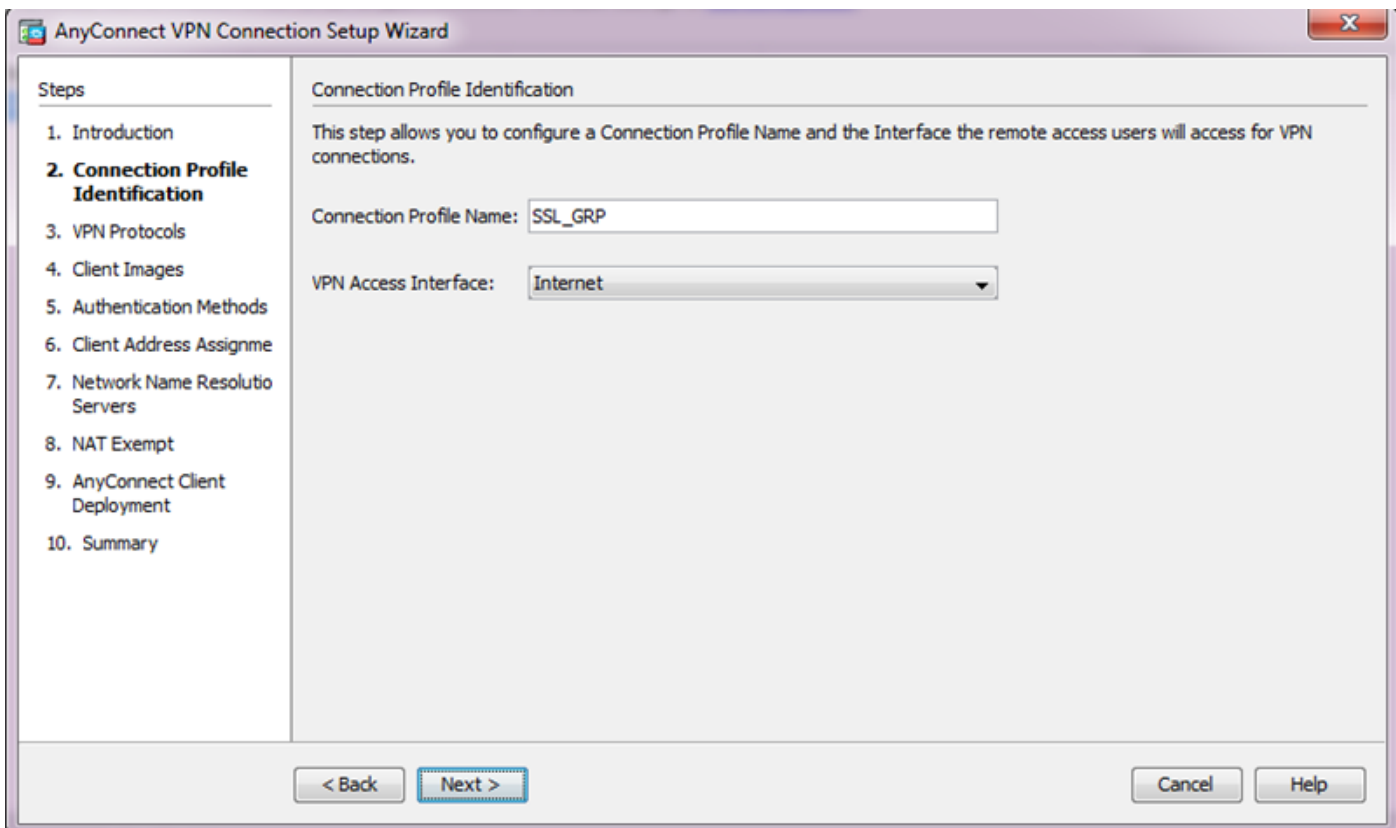
A configuração Wizard/CLI de AnyConnect pode ser usada a fim configurar o cliente seguro da mobilidade de AnyConnect. Assegure-se de que um pacote do cliente de AnyConnect esteja transferido arquivos pela rede ao flash/disco do Firewall ASA antes que você continue.

Termine estas etapas a fim configurar o cliente seguro da mobilidade de AnyConnect através do wizard de configuração:

1. O log no ASDM e navega aos **wizard VPN de Wizards>>** ao **wizard VPN de AnyConnect** para lançar o wizard de configuração e a clicá-los **em seguida**.

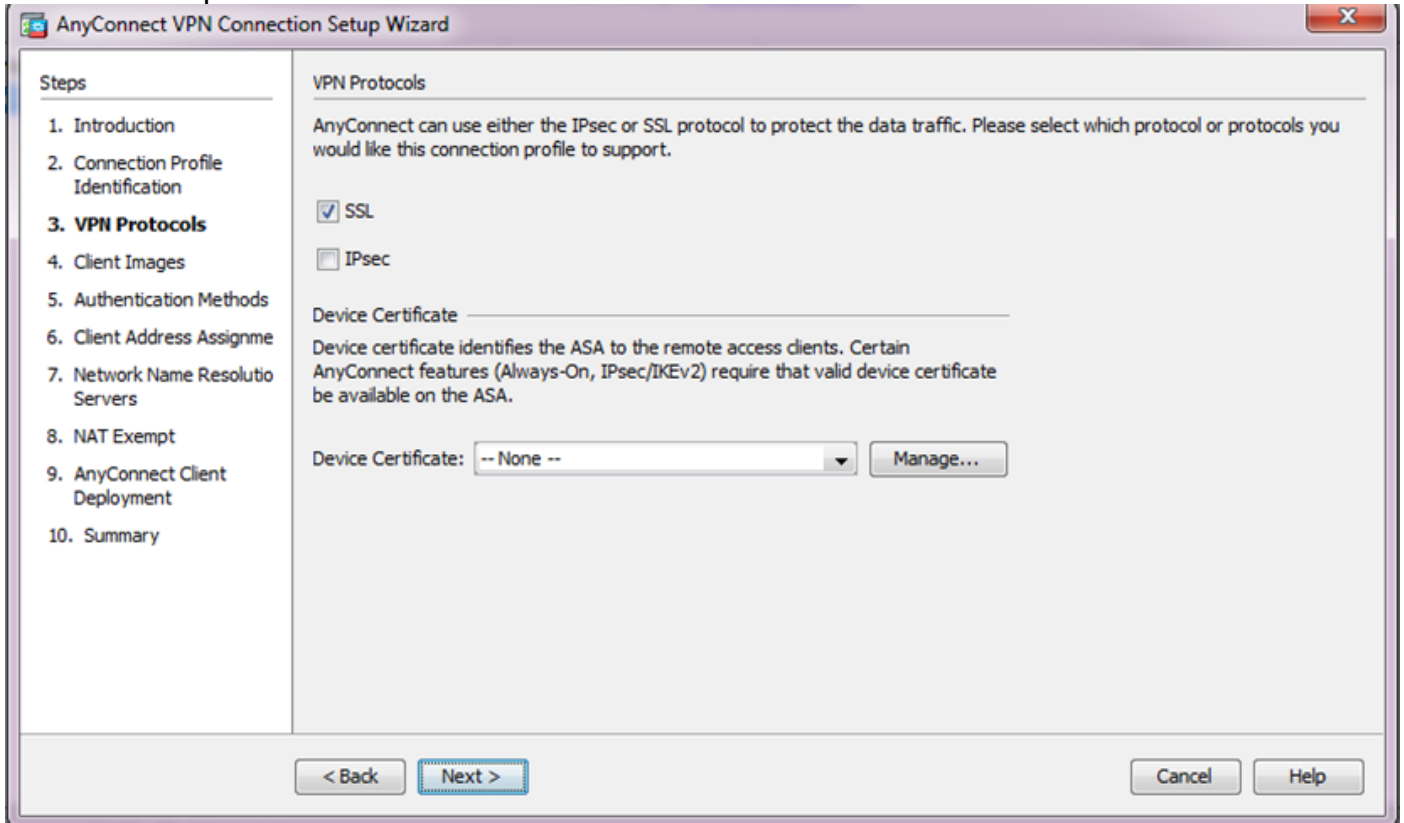


2. Dê entrada com o nome do perfil de conexão, escolha a relação em que o VPN será terminado da interface de acesso VPN deixa cair para baixo o menu, e o clica **em seguida**.



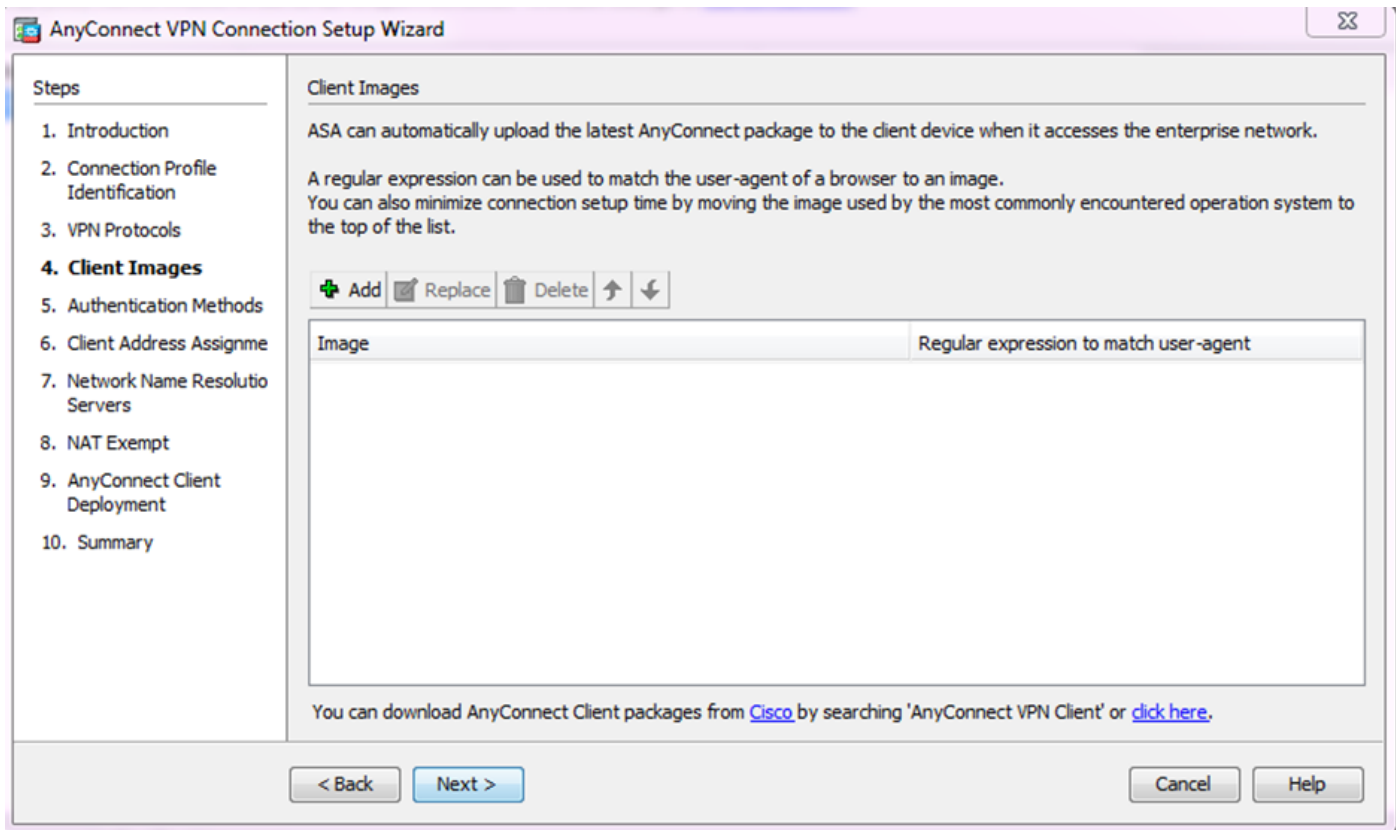
3. Verifique a caixa de verificação **SSL** a fim permitir o secure sockets layer (SSL). O certificado do dispositivo pode ser um certificado emitido Certificate Authority (CA) confiada da terceira parte (tal como Verisign, ou confie), ou um certificado auto-assinado. Se o certificado é instalado já no ASA, a seguir pode ser escolhido através do menu de gota para baixo.

1. Nota: Este certificado é o certificado do lado de servidor que será apresentado pelo ASA aos clientes SSL. Se não há nenhum certificado de servidor instalado atualmente no ASA do que um certificado auto-assinado deve ser gerado, a seguir clique **controlam**.A fim instalar um certificado da terceira, termine as etapas que são descritas no [ASA 8.x instalam manualmente Certificados do vendedor da 3ª parte para o uso com documento Cisco do exemplo de configuração WebVPN](#).Permita o **certificado dos protocolos** e do **dispositivo VPN**.Clique em Next.

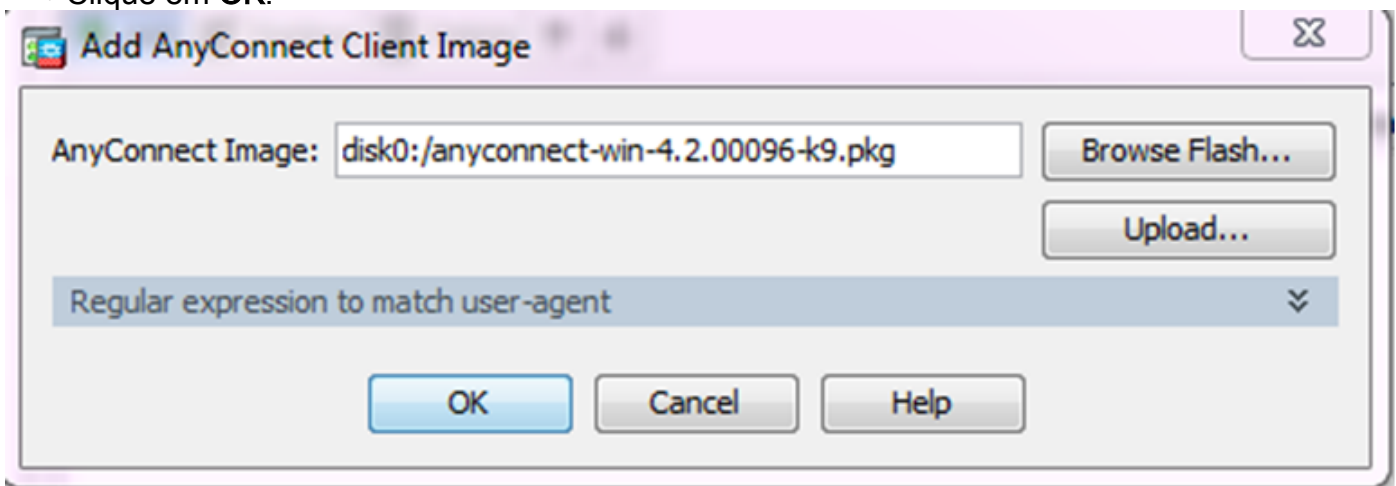


4. O clique **adiciona** a fim adicionar o pacote do cliente de AnyConnect (arquivo .package) da unidade local ou do flash/disco do ASA.

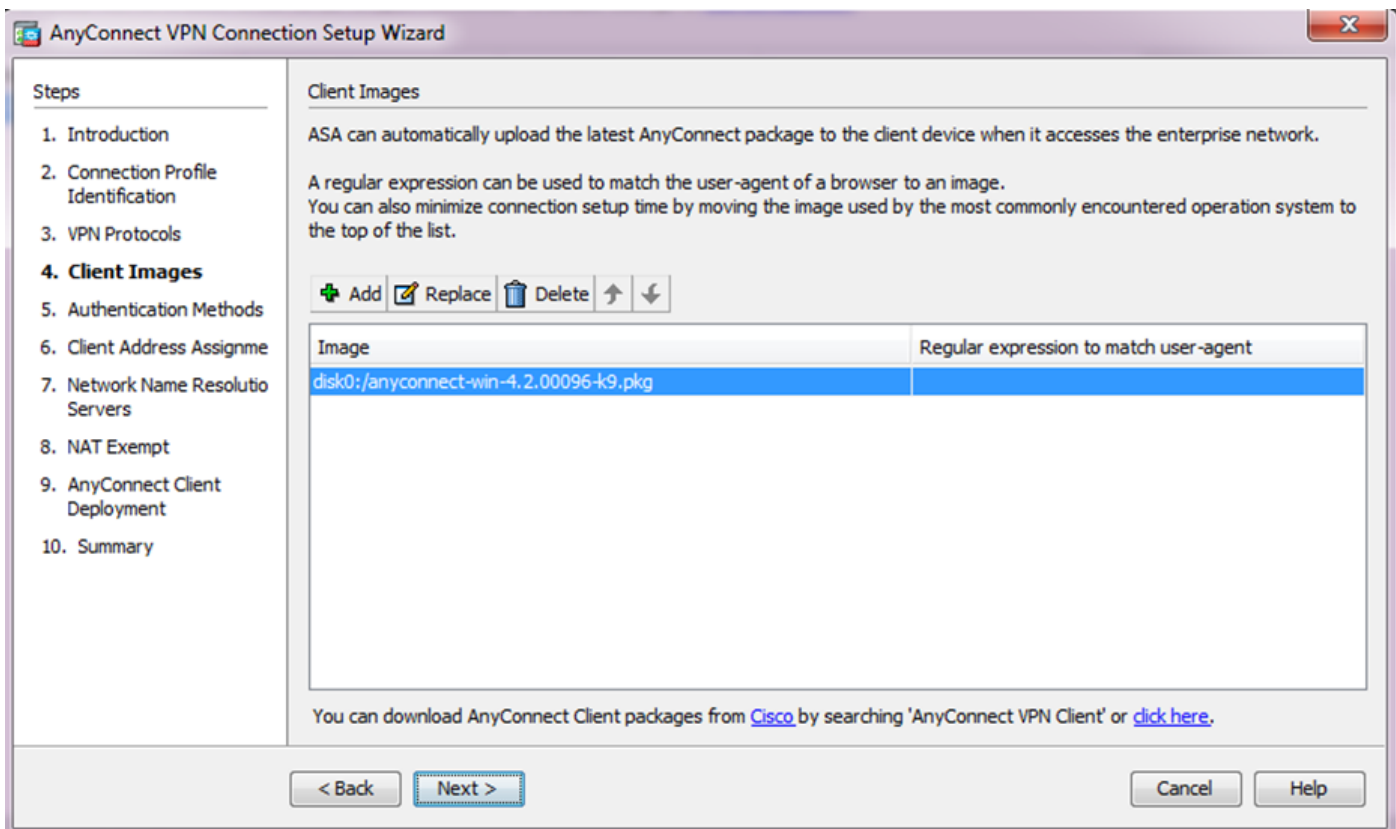
O clique **consulta o flash** a fim adicionar a imagem da movimentação instantânea, ou a **transferência de arquivo pela rede** do clique a fim adicionar a imagem da unidade local de máquina host.



- Você poderia transferir arquivos pela rede o arquivo AnyConnect.pkg do flash ASA/disco (se o pacote é já lá) ou da unidade local.
- Consulte o flash – para selecionar o pacote de AnyConnect do flash/disco ASA.
- Transferência de arquivo pela rede – para selecionar o pacote de AnyConnect da unidade local de máquina host.
- Clique em **OK**.

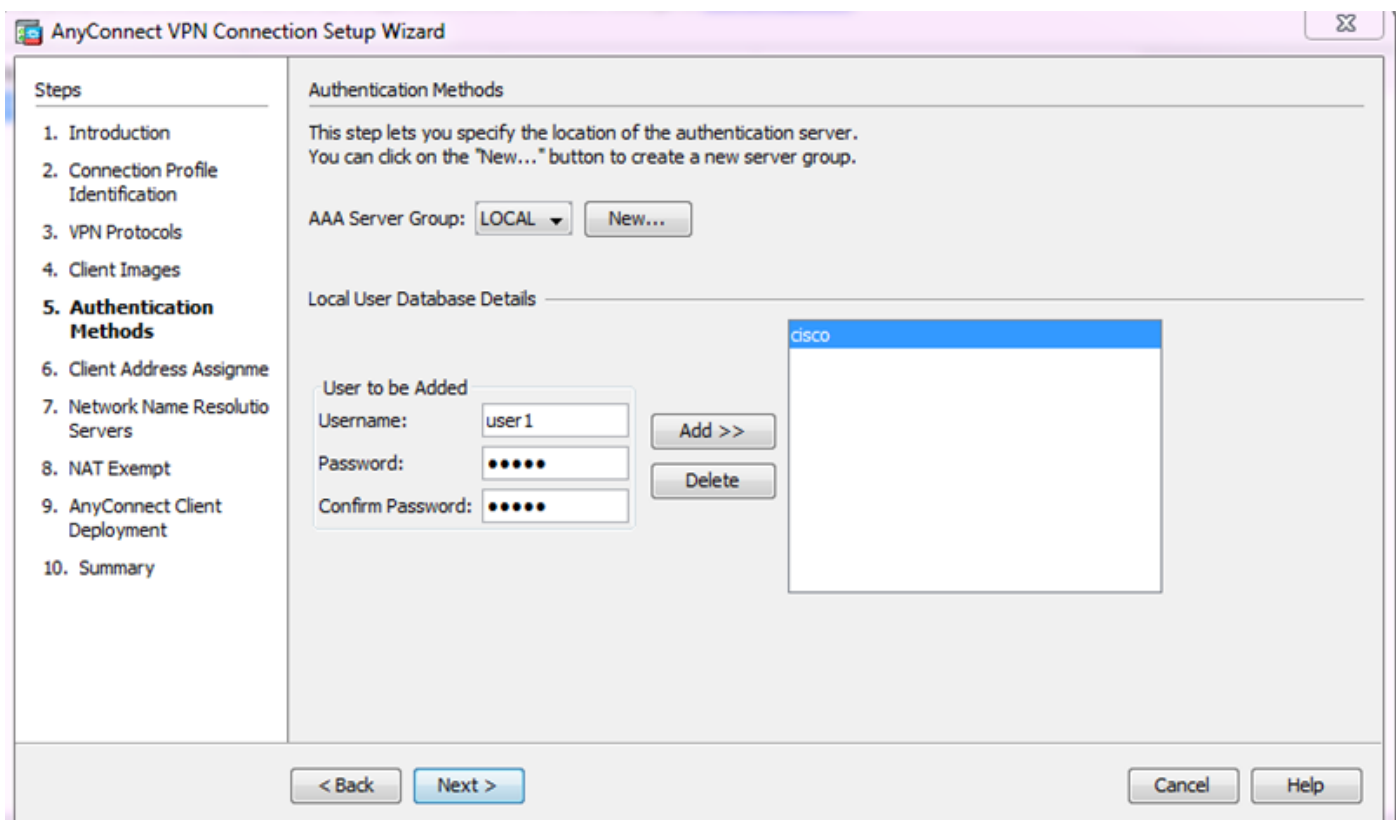


- Clique em Next.

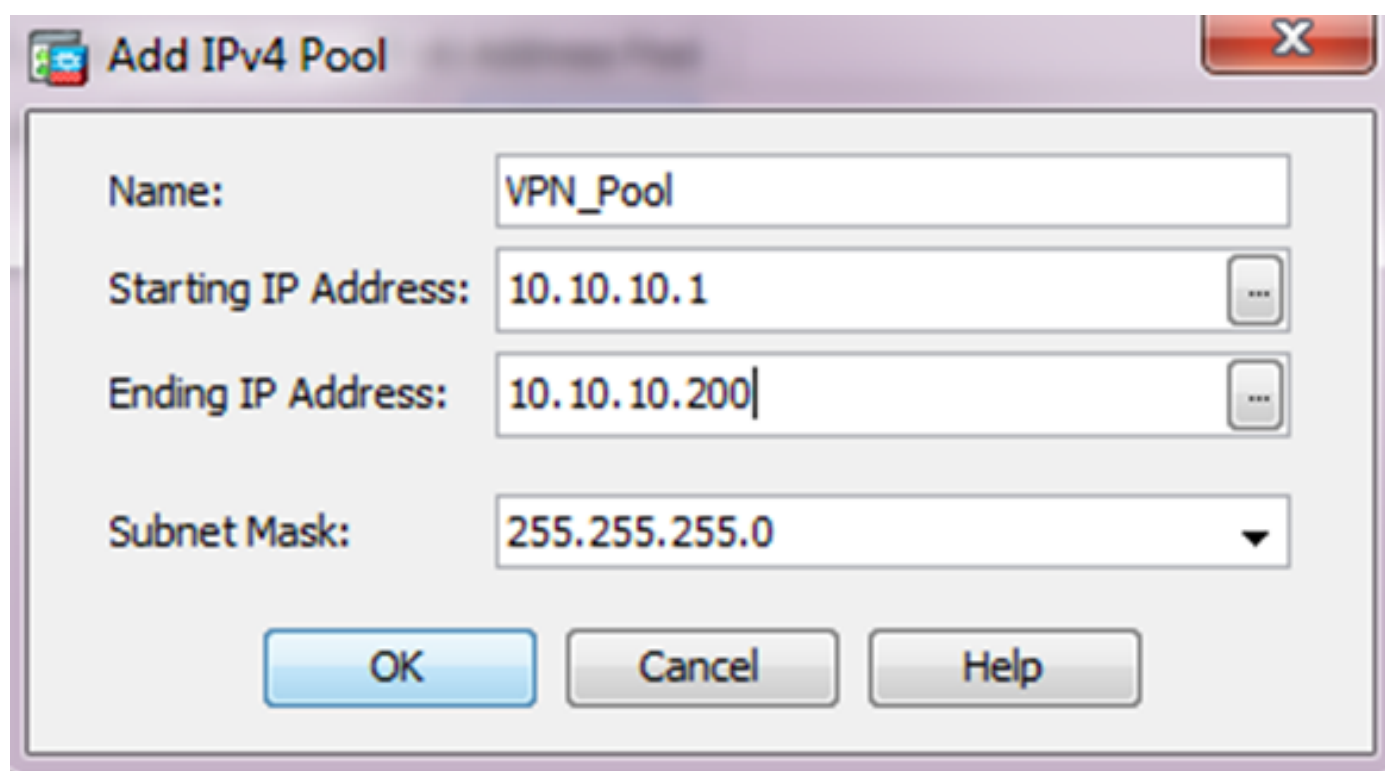
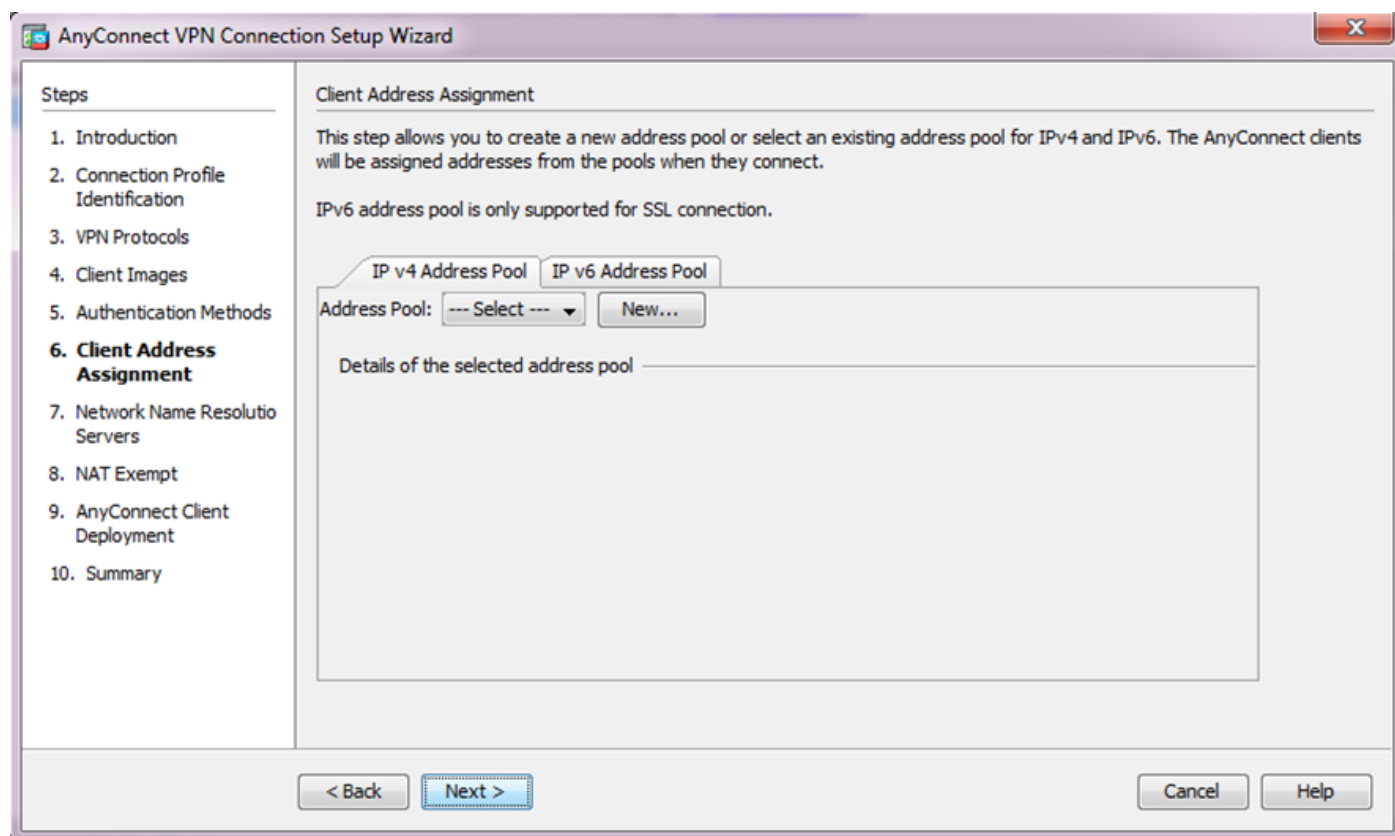


5. A autenticação de usuário pode ser terminada através dos grupos de servidor do Authentication, Authorization, and Accounting (AAA). Se os usuários são configurados já, a seguir escolha o **LOCAL** e clique-o **em seguida**. Mais adicionar um usuário à base de dados de usuário local e clique-o **em seguida**.

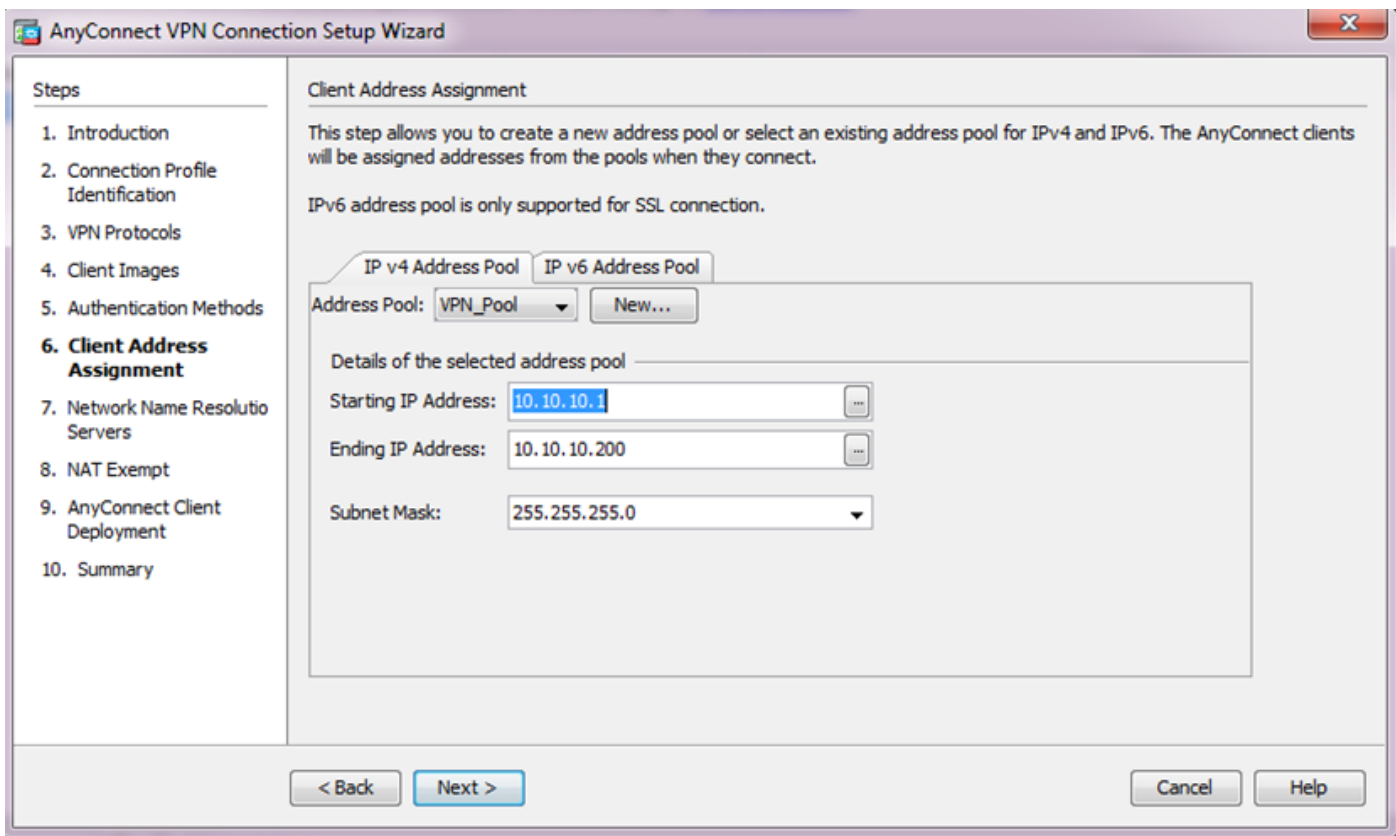
Nota: Neste exemplo, a **autenticação local** é configurada, assim que significa que a base de dados de usuário local no ASA estará usada para a autenticação.



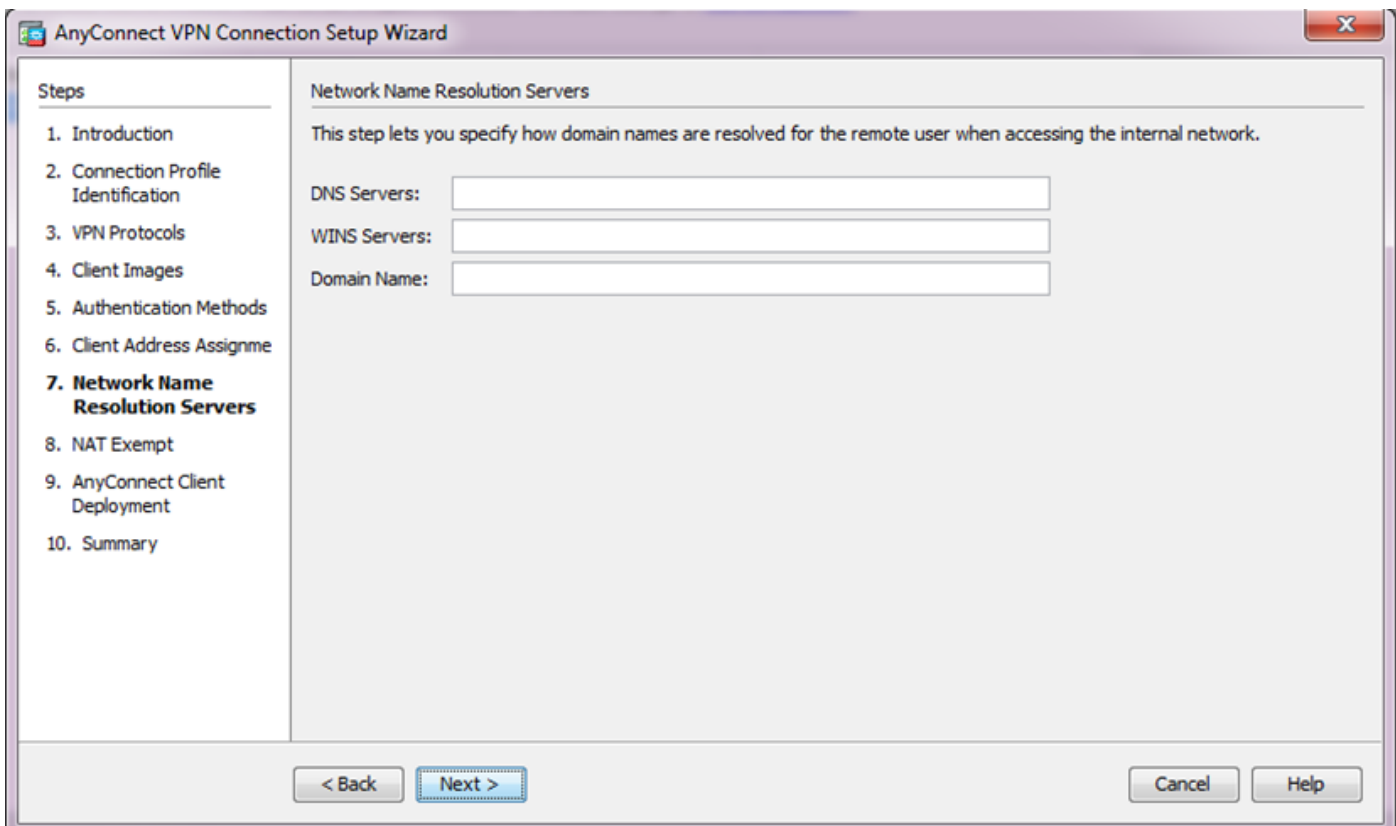
6. Assegure-se de que o conjunto de endereços para os clientes VPN esteja configurado. Se um pool IP é configurado já então selecione-o do menu de gota para baixo. Se não, clique **novo** a fim configurar. Uma vez que completo, clique **em seguida**.



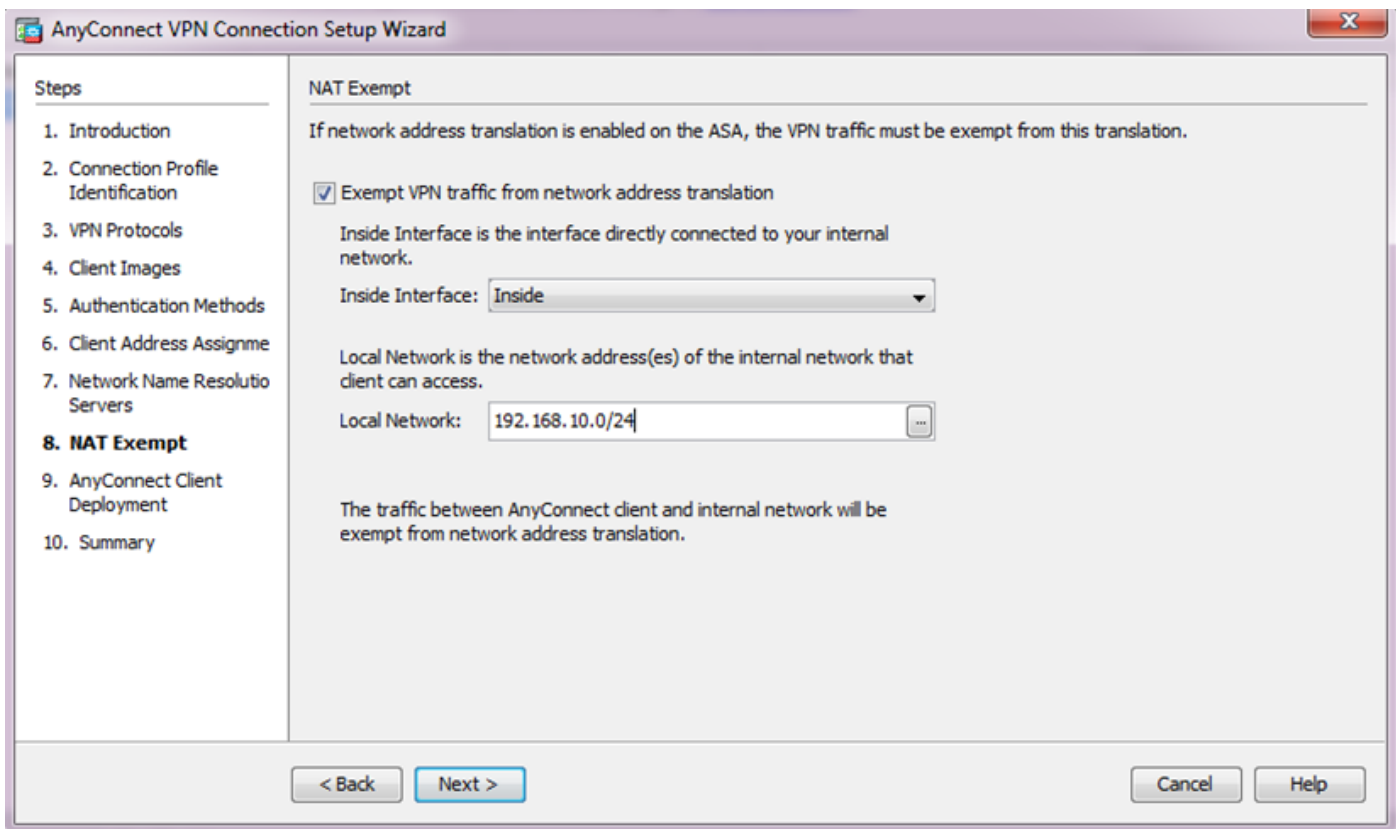
- Clique em Next.



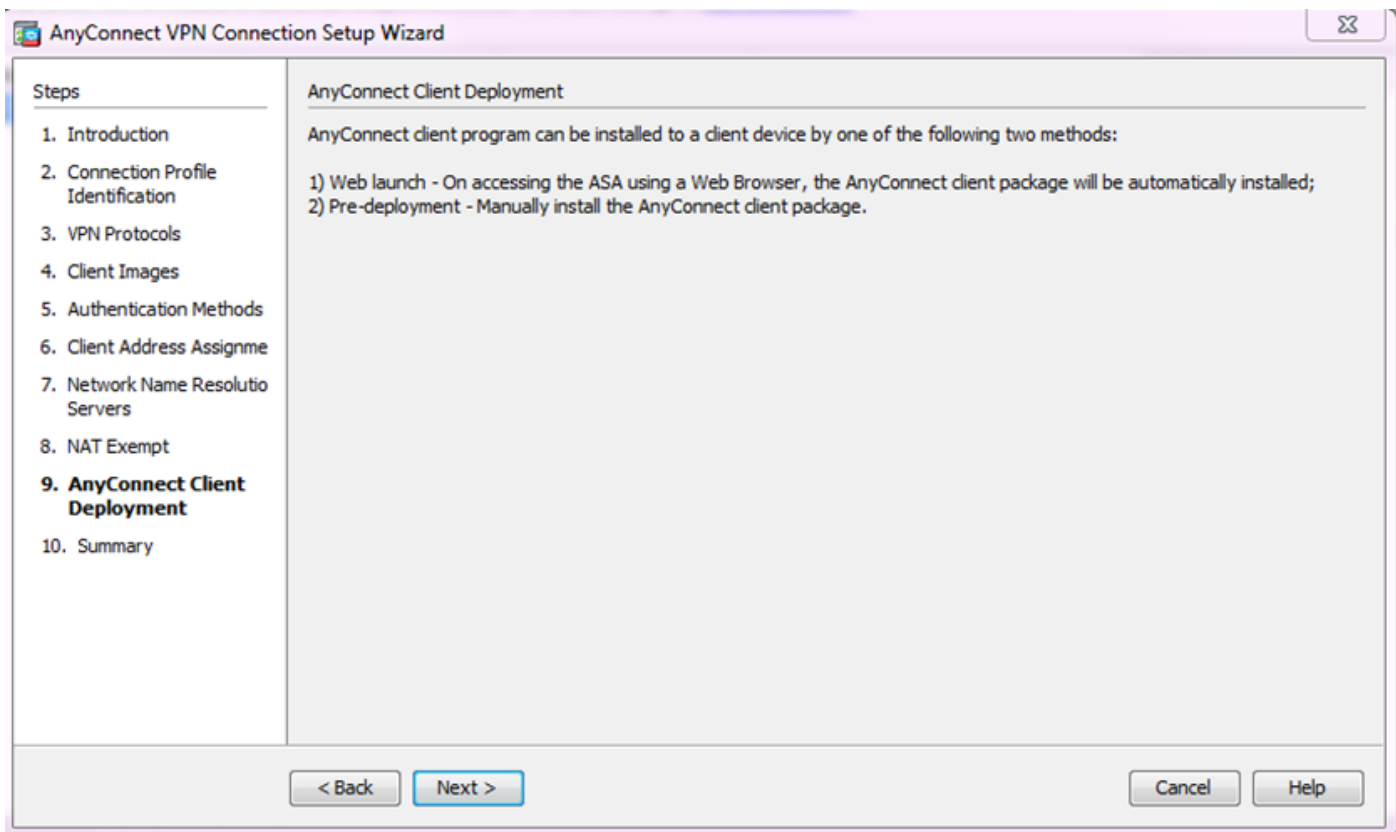
7. Opcionalmente, configurar os server do Domain Name System (DNS) e o DNS nos campos DNS e de Domain Name, e clique-os então **em seguida**.



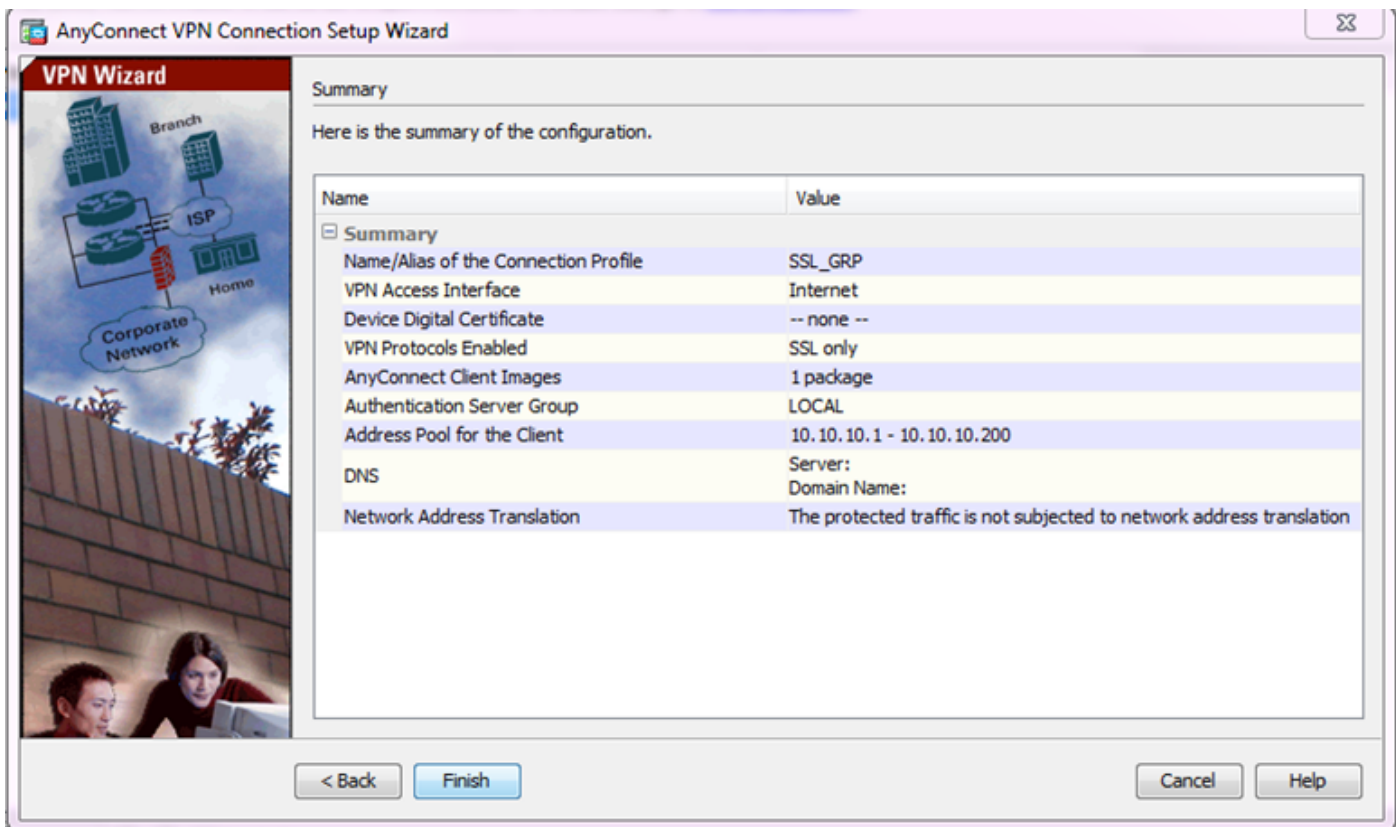
8. Assegure-se de que o tráfego entre o cliente e a sub-rede interna deva estar isento de toda a tradução de endereço de rede dinâmica (NAT). Permita o **tráfego isento VPN** da caixa de verificação da **tradução de endereço de rede** e configure a interface de LAN que será usada para a isenção. Também, especifique a rede local que deve ser isentada e clique **em seguida**.



9. Clique em Next.

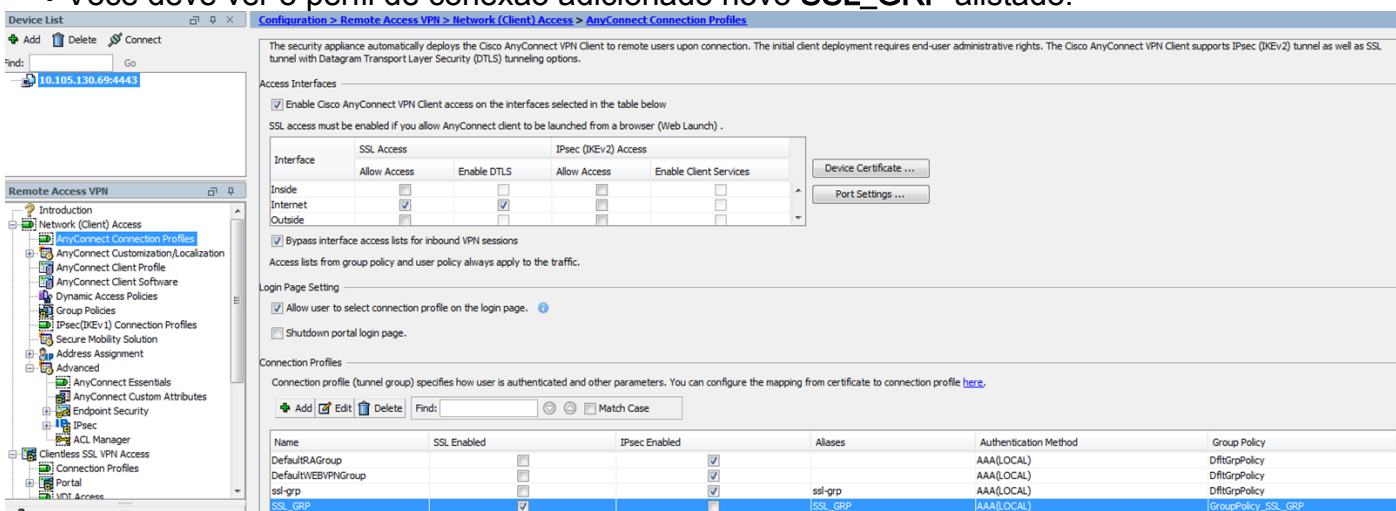


10. A etapa final mostra o sumário, **revestimento do clique** para terminar a instalação.

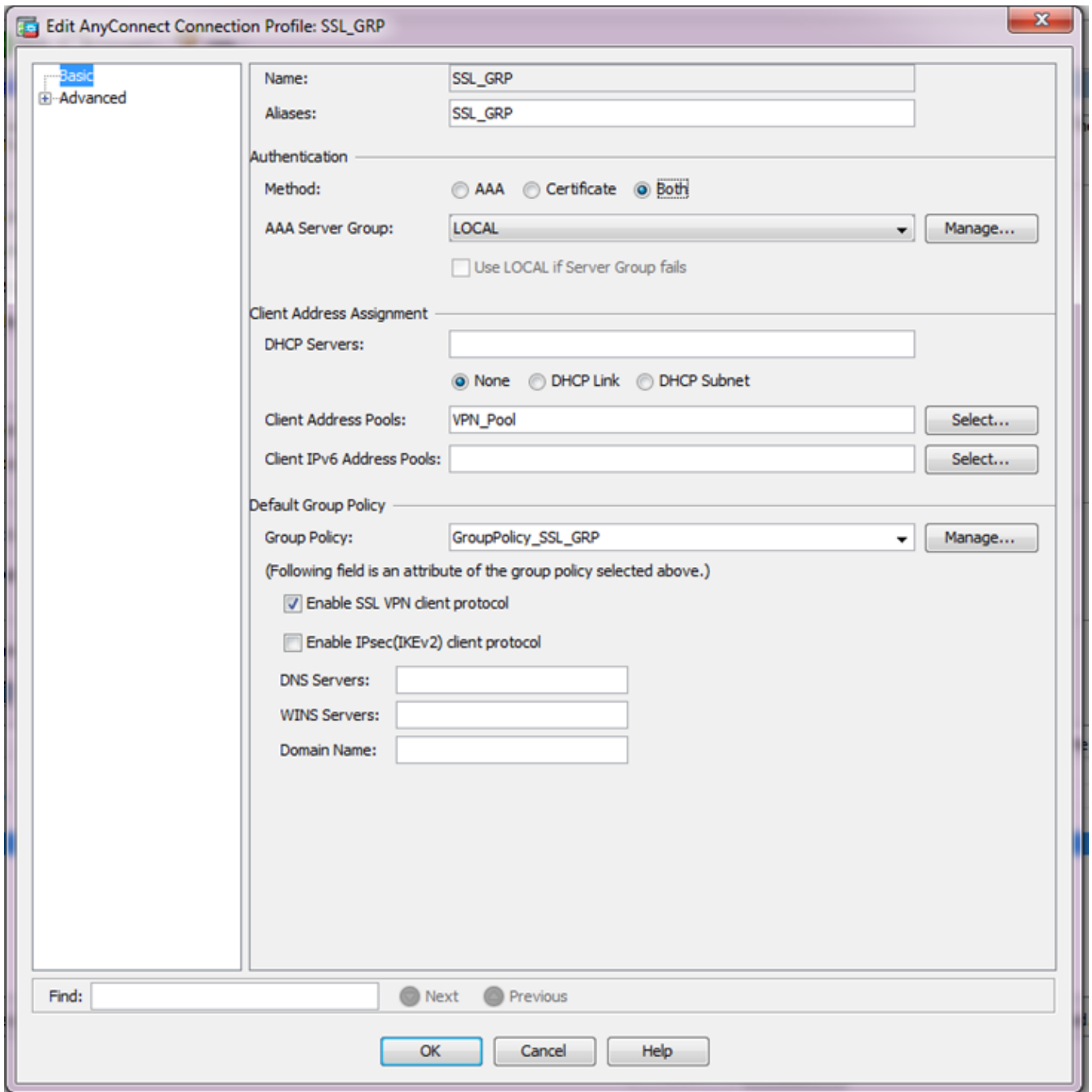


A configuração de cliente de AnyConnect está agora completa. Contudo, quando você configura AnyConnect através do wizard de configuração, configura o método de autenticação como o AAA à revelia. A fim autenticar os clientes através dos Certificados e do username/senha, o grupo de túneis (perfil de conexão) deve ser configurado para usar Certificados e AAA como o método de autenticação.

- Navegue à configuração > ao acesso do acesso remoto VPN > da rede (cliente) > aos perfis de conexão de AnyConnect.
- Você deve ver o perfil de conexão adicionado novo **SSL_GRP** alistado.



- A fim configurar o AAA e o certificado de autenticação, para selecionar o perfil de conexão **SSL_GRP** e o clique edite.
- Sob o método de autenticação, selecione ambos.



Configurar o CLI para AnyConnect

!! *****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 mb02jYs13AXlIAGa 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Nota: A [ferramenta Output Interpreter \(exclusiva para clientes registrados\)](#) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Assegure-se de que o server CA esteja permitido.

mostre o server cripto Ca

```
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!!
```

Assegure-se de que esteja permitido ao usuário o registro após adicionar:

*****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

Você pode verificar os detalhes da conexão do anyconnect através do CLI ou do ASDM.

Através do CLI

mostre o anyconnect do detalhe VPN-sessiondb

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 :

Através do ASDM

- Navegue à **monitoração > VPN > estatísticas de VPN > sessões.**
- Escolha o **filtro** como por **todo o Acesso remoto.**
- Você pode executar qualquer uma das ações para o cliente selecionado de AnyConnect.

Os detalhes fornecem mais informação sobre a sessão

Logout- para logout manualmente o usuário do final do cabeçalho

Sibile para sibilar o cliente de AnyConnect do final do cabeçalho

Username	Group Policy Connection Profile	Public IP Address Assigned IP Address	Protocol Encryption	Login Time Duration	Bytes Tx Bytes Rx	Details
user1	ssl-pool ssl-grp	10.142.189.80 192.168.1.1	AnyConnect-Parent-SSL-Tunnel-DTLS- AnyConnect-Parent:(1)none-SSL-Tu...	14:39:08 UTC Mo... 0h:00m:33s	10998 885	Logout Ping

Troubleshooting

Esta seção fornece informações que você pode usar na solução de problemas de sua

configuração.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

Cuidado: No ASA, você pode ajustar-se vários níveis de depuração; à revelia, o nível 1 é usado. Se você muda o nível de depuração, a verbosidade da depuração pode aumentar. Faça isto com cuidado, especialmente nos ambientes de produção.

- **debug crypto ca**
- **server do debug crypto ca**
- **mensagens do debug crypto ca**
- **transações do debug crypto ca**
- **debugar o anyconnect do webvpn**

Este resultado do debug mostra quando o server CA é permitido usando o comando **no shut**.

```
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!

Este resultado do debug mostra o registro do cliente

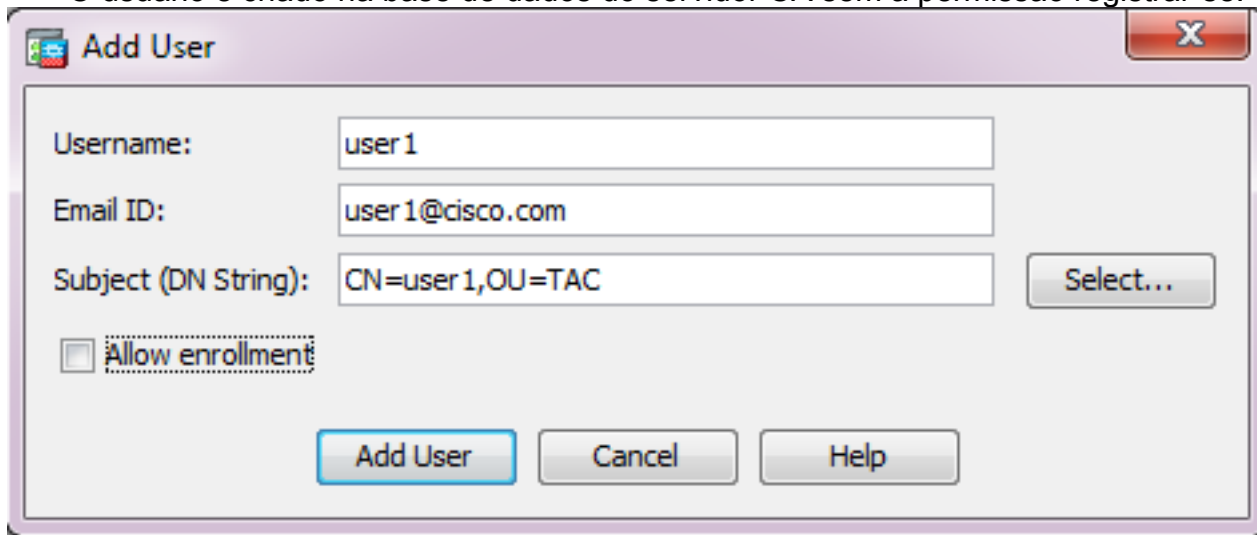
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255

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
```

O registro do cliente pode falhar sob estas condições:

Encenação 1.

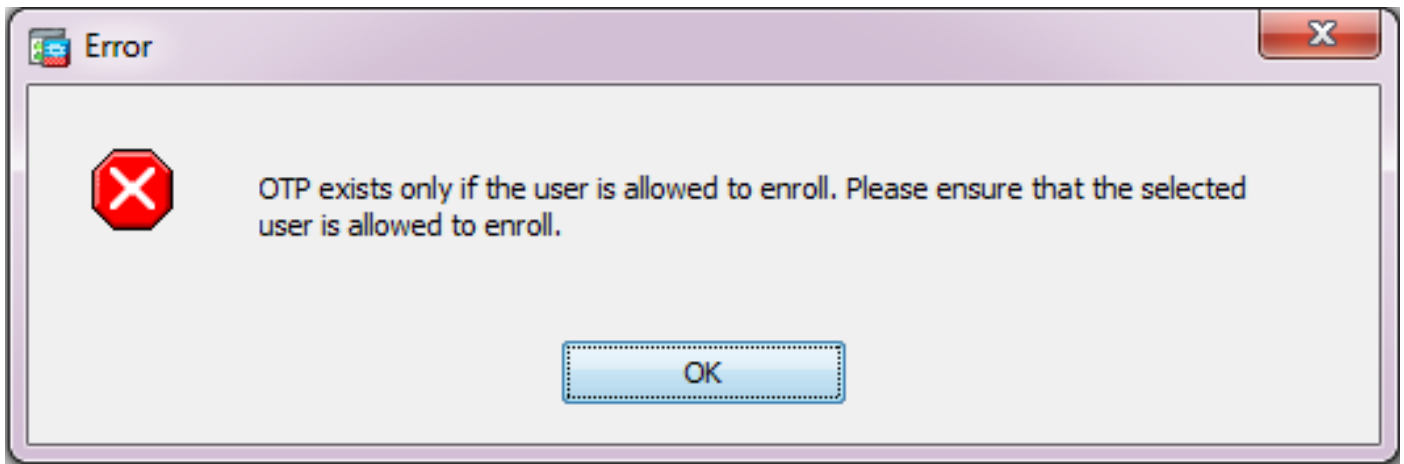
- O usuário é criado na base de dados do servidor CA sem a permissão registrar-se.



Equivalente CLI:

```
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
```

- No caso onde não é permitido ao usuário se registrar, tentando gerar/email o OTP para o usuário gere esta Mensagem de Erro.



Cenário 2.

- Verifique a porta e conecte-a em qual o portal do registro está disponível usando o comando **webvpn** da corrida da mostra. A porta padrão é 443 mas pode ser alterada.
- Assegure-se de que o cliente tenha a alcançabilidade de rede ao **IP address da relação** em que o **webvpn** é permitido na porta usada para alcançar com sucesso o portal do registro.

O cliente pode não alcança o portal do registro do ASA nesses casos:

1. Se qualquer dispositivo intermediário obstrui as conexões recebidas do cliente ao IP do **webvpn** do ASA na porta especificada.
2. O estado da relação está para baixo em que **webvpn** é permitido.

- Esta saída mostra que o portal do registro está disponível no **IP address do Internet da relação na porta** feita sob encomenda **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
```

Cenário 3.

- O local padrão do armazenamento da base de dados do servidor CA é memória Flash do ASA.
- Assegure-se de que a memória Flash tenha o espaço livre para gerar e salvar o arquivo do **pkcs12** para o usuário durante o registro.
- No caso onde a memória Flash não tem bastante espaço livre, o ASA não termina o processo do registro do cliente e gere estes debug logs:

```
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

Informações Relacionadas

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Guia de solução de problemas do cliente AnyConnect VPN - Problemas comuns](#)
- [Controlando, monitorando, e pesquisando defeitos sessões de AnyConnect](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)