Configure el ASA como un servidor local de CA y headend de AnyConnect

Contenido

Introducción

Este documento describe cómo poner un dispositivo de seguridad adaptante de Cisco (ASA) como servidor del Certificate Authority (CA) y como gateway de Secure Sockets Layer (SSL) para los Clientes de movilidad Cisco AnyConnect Secure.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración básica ASA que funciona con la versión de software 9.1.x
- ASDM 7.3 o más alto

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 5500 Series ASA que funcionan con la versión de software 9.1(6)
- Versión de cliente segura 4.x de la movilidad de AnyConnect para Windows
- PC que ejecuta un OS soportado por la carta de la compatibilidad.
- Versión 7.3 del Cisco Adaptive Security Device Manager (ASDM)

Note: Descargue el paquete de AnyConnect VPN Client (anyconnect-win*.pkg) de Descarga de Cisco Software (sólo clientes registrados). Copie el AnyConnect VPN client en la memoria flash ASA, que será descargada a los equipos de los usuarios remotos para establecer la conexión SSL VPN con el ASA. Consulte la sección Instalación de AnyConnect Client de la guía de configuración ASA para obtener más información.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El Certificate Authority en el ASA proporciona estas funciones:

- Integra la operación básica del Certificate Authority en el ASA.
- Despliega los Certificados.
- Proporciona marcar seguro de la revocación de los Certificados publicados.
- Proporciona un Certificate Authority en el ASA para el uso con las conexiones VPN del navegador-based(WebVPN) y del cliente-based(AnyConnect) SSL.
- Provides confiaba en los Certificados digitales a los usuarios, sin la necesidad de confiar en la autorización externa del certificado.
- Proporciona una autoridad segura, interna para la autenticación certificada y una inscripción directa del usuario de las ofertas mediante un login del sitio web.

Guías de consulta y limitaciones

- Soportado en el modo firewall ruteado y transparente.
- Solamente un en un momento del servidor de CA del local puede ser residente en un ASA.
- El ASA como característica local del servidor de CA no se soporta en una configuración de la Conmutación por falla.
- El ASA a partir ahora de la actuación como servidor local de CA soporta solamente la generación de los Certificados SHA1.
- El servidor local de CA se puede utilizar para las conexiones VPN basadas en buscador y basadas en el cliente SSL. No soportado actualmente para el IPSec.
- No soporta el Equilibrio de carga VPN para CA local.
- CA local no puede ser un subordinado a otro CA. Puede actuar solamente como raíz CA.
- El ASA no puede alistar actualmente a CA el servidor local para el certificado de identidad.
- Cuando se completa una inscripción del certificado, el ASA salva un archivo del PKCS12 que contiene el keypair y la Cadena de certificados del usuario, que requiere cerca de 2 KB de memoria flash o de espacio en disco por la inscripción. La cantidad real de espacio en disco depende de los campos configurados del tamaño de clave y del certificado RSA. Tenga esta guía de consulta presente al agregar un gran número de inscripciones del certificado pendientes en un ASA con las cantidades limitadas de memoria flash disponible, porque

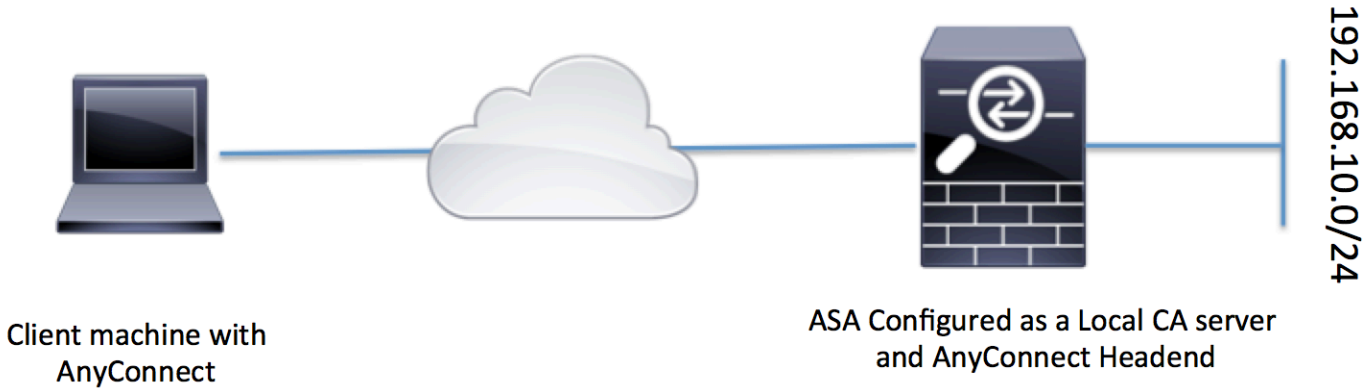
estos archivos del PKCS12 se salvan en memoria flash para la duración del descanso configurado de la extracción de la inscripción.

Configurar

Esta sección describe cómo configurar Cisco ASA como servidor local de CA.

Note: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red



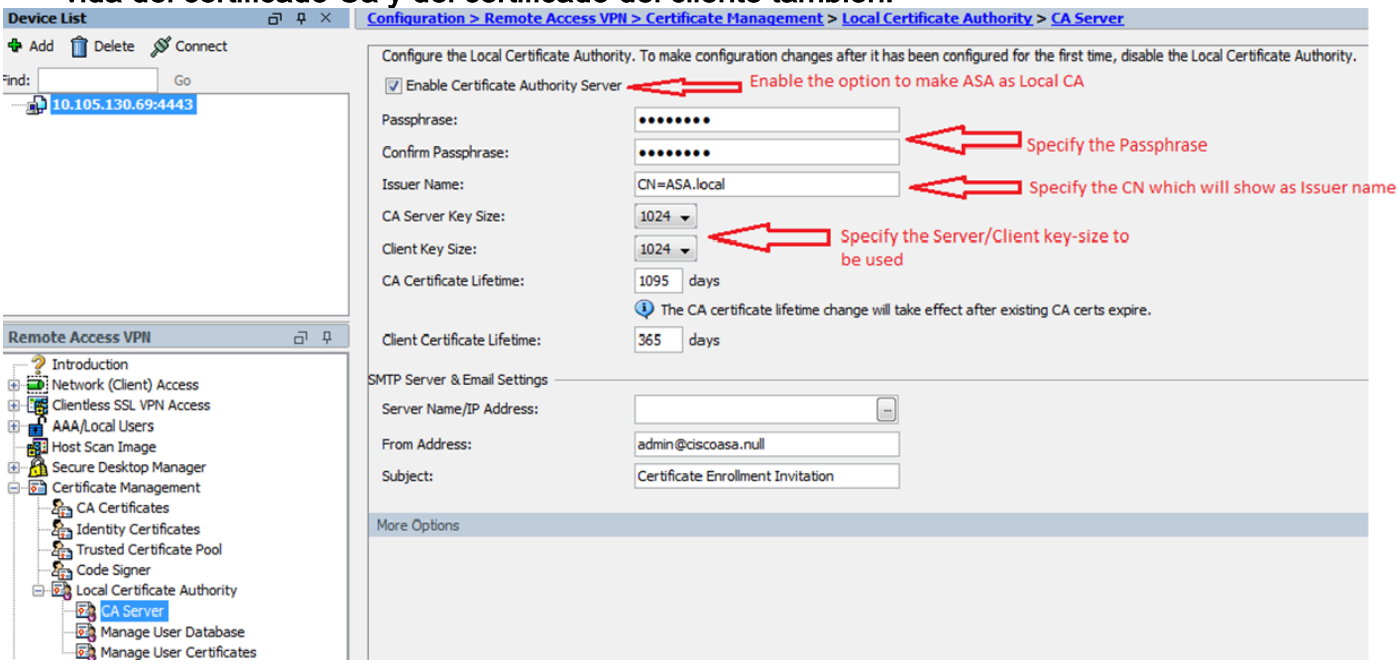
ASA como servidor local de CA

Paso 1. Configure y habilite el servidor local de CA en el ASA

- Navegue al **Certificate Management (Administración de certificados) de la configuración > del VPN de acceso remoto > Certificate Authority local > servidor de CA**. Marque la **opción del servidor del Certificate Authority del permiso**.
- Configure el passphrase. El passphrase debe ser un mínimo, 7 caracteres que se utiliza para codificar y para salvar un archivo del PKCS12 que incluya el certificado de CA y el par clave locales. El passphrase desbloquea el archivo del PKCS12 si se pierde el certificado de CA o el keypair.
- Configure el nombre del emisor. Este campo aparecería como certificado raíz CN. Esto se puede especificar en el formato siguiente: CN (Common Name), OU (unidad de la organización), (o) organización, L (lugar), S (estado) y C (país).
- **Configuración opcional:** Configure al servidor SMTP y las configuraciones del servidor de correo electrónico para asegurar el OTP se podrían recibir para terminar a los clientes vía el correo para completar la inscripción. Usted puede configurar el nombre de host o la dirección IP de su servidor local Email/SMTP. Usted puede también configurar del **direccionamiento** y

del **campo Subject del** correo electrónico que los clientes recibirían. Por abandono, del direccionamiento es el **admin@<ASA hostname>.null y el tema es invitación de la inscripción del certificado.**

- **Configuración opcional:** Usted puede configurar los parámetros optativos como el **tamaño del tamaño de clave del cliente, de la clave del servidor de CA, el curso de la vida del curso de la vida del certificado Ca y del certificado del cliente también.**



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
```

Éstos son los campos adicionales que se podrían configurar bajo Configuración del servidor local de CA.

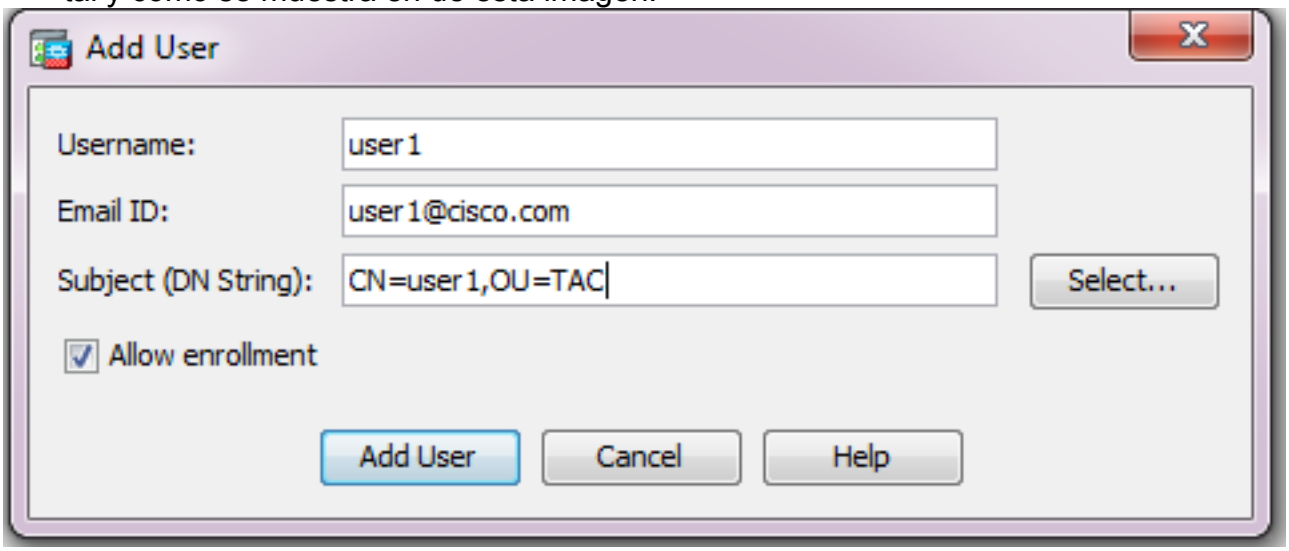
CRL Distribution Point URL	Ésta es la ubicación CRL en el ASA. La ubicación predeterminada es http://hostname.domain/+CSCOCA+/asa_ca.crl pero el URL podría ser modificado.
Interfaz Publicar-CRL y puerto	Para hacer el CRL disponible para el HTTP descargue en una interfaz dada y el puerto, elige una interfaz publicar-CRL de la lista desplegable. Entonces ingrese el número del puerto, que puede ser cualquier número del puerto a partir de la 1-65535. **El número del puerto predeterminado es el puerto TCP 80.**
Vida útil de CRL	CA local pone al día y reedita el CRL cada vez que un Certificado de usuario es revocado o unrevoked, pero si hay ninguna revocación cambia, el CRL se reedita automáticamente una vez que cada vida útil de CRL, el período de tiempo que usted

	especifica con el **crlcommand del curso de la vida** durante la configuración local de CA. Si usted no especifica una vida útil de CRL, el período del tiempo predeterminado es **seis horas**.
Ubicación de almacenamiento de la base de datos	El ASA accede y implementa la información del usuario, los Certificados publicados, y las listas de revocación usando una base de datos local CA. **Esta base de datos reside en memoria flash local por abandono**, o se puede configurar para residir en un sistema del archivo externo que sea montado y accesible al ASA.
Asunto predeterminado	Ingrese un tema predeterminado (cadena DN) para añadir al final del fichero a un nombre de usuario en los Certificados publicados. Los atributos permitidos DN se proporcionan en esta lista: • CN (Common Name) SN (apellido) • O (nombre de la organización) • L (lugar) • C (país) • OU (unidad de la organización) • EA (dirección de correo electrónico) • ST (estado/provincia) • T (título)
Período de inscripción	Establece el límite de tiempo de la inscripción en las horas dentro de las cuales el usuario podría extraer el archivo del PKCS12 del ASA. El valor predeterminado es 24 horas. **Note**: Si expira el período de inscripción antes de que el usuario extraiga el archivo del PKCS12 que incluye el Certificado de usuario, la inscripción no se permite.
Un vencimiento de contraseña del tiempo	Define la cantidad de tiempo en las horas que el OTP es válido para la inscripción del usuario. Este período de tiempo comienza cuando se permite al usuario alistar. El valor del defaut es 72 horas.
Recordatorio del vencimiento del certificado	Especifica el número de días antes de que expire el certificado que un recordatorio inicial al reenroll está enviado para certificar a los propietarios.

Paso 2. Cree y agregue a los usuarios a la base de datos ASA

- Navegue al **Certificate Management (Administración de certificados) de la configuración > del VPN de acceso remoto > Certificate Authority local > manejan al usuario que Database.Click agregan**.

- Especifique al usuario detalla viz el nombre de usuario, el correo electrónico ID y el asunto, tal y como se muestra en de esta imagen.

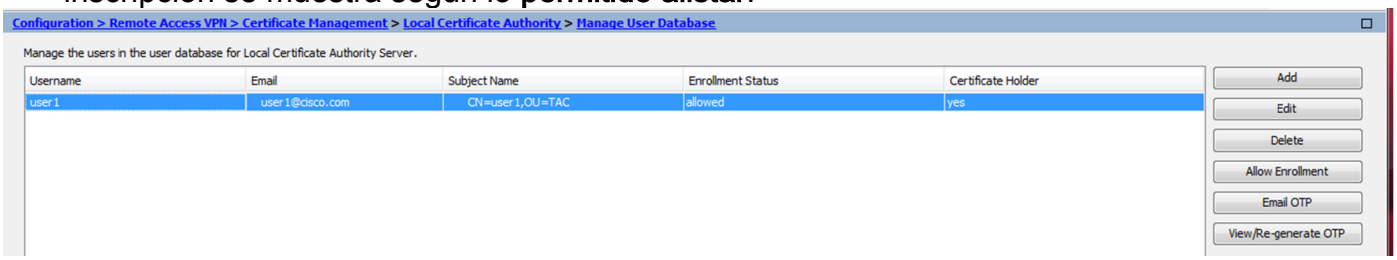


- Asegúrese que **permite** se marca la **inscripción** para usted permitir que aliste para el certificado.
- El tecleo **agrega al usuario** para completar la configuración de usuario.

Equivalente CLI:

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

- Después de que agreguen al usuario a la base de datos de usuarios, el estatus de la inscripción se muestra según lo **permitido alistar**.



CLI para verificar el estatus del usuario:

```
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
```

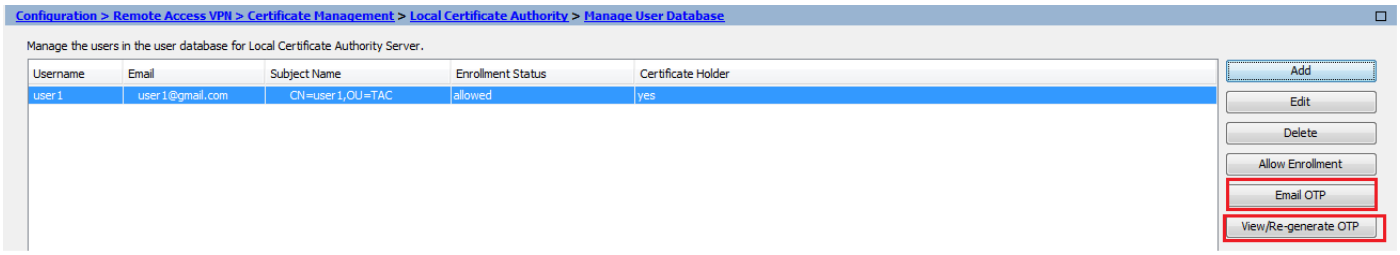
- Después de que hayan agregado al usuario a la base de datos de usuarios, la una contraseña del tiempo (OTP), para que el usuario complete la inscripción, se puede proporcionar usando cualquiera esto:

Envíe por correo electrónico el OTP (requiere las configuraciones del servidor SMTP y del correo electrónico que se configurarán bajo Configuración del servidor de CA).

O

Vea directamente el OTP y la parte con el usuario haciendo clic en View/Re-generate OTP. Esto

se puede también utilizar al regenrate el 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
```

Paso 3. Webvpn del permiso en la interfaz de WAN

- Acceso Web del permiso en el ASA para que clientes pidan para la inscripción.

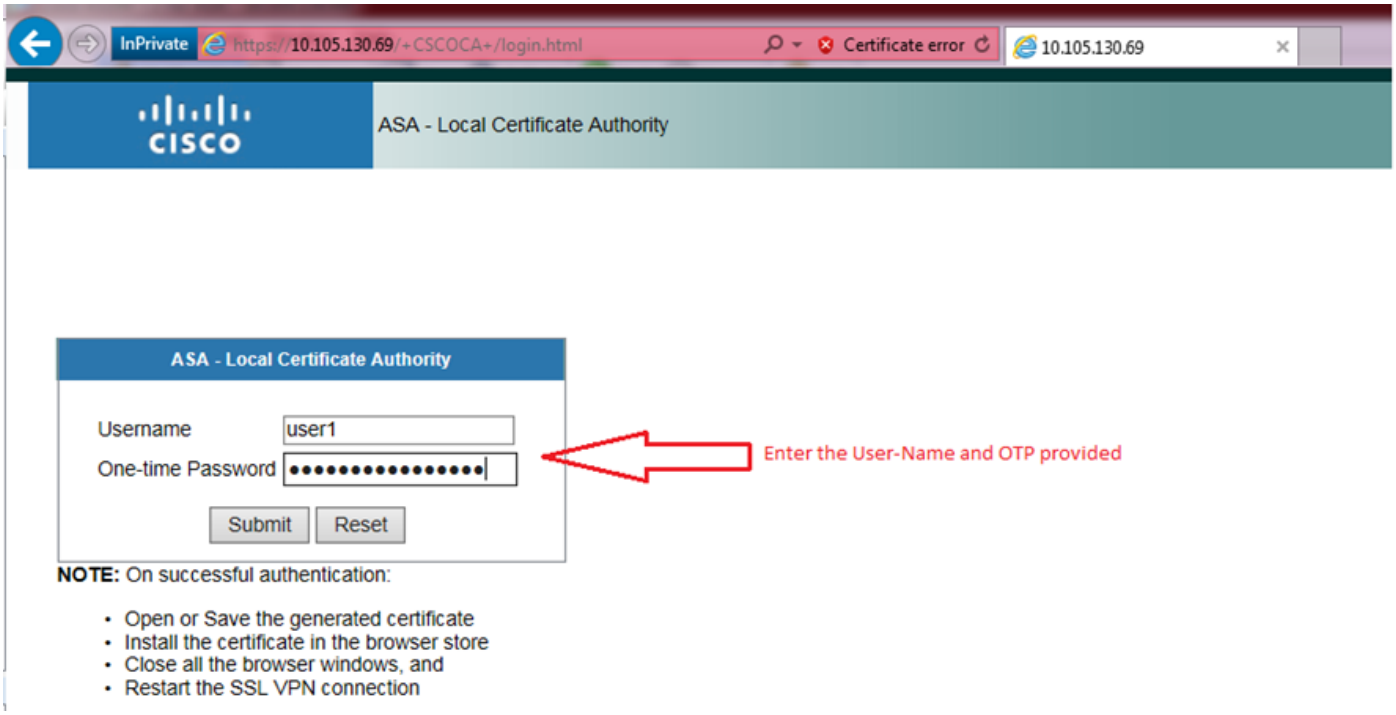
```
ASA# show crypto ca server user-db
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

Paso 4. Importe el certificado en la máquina del cliente

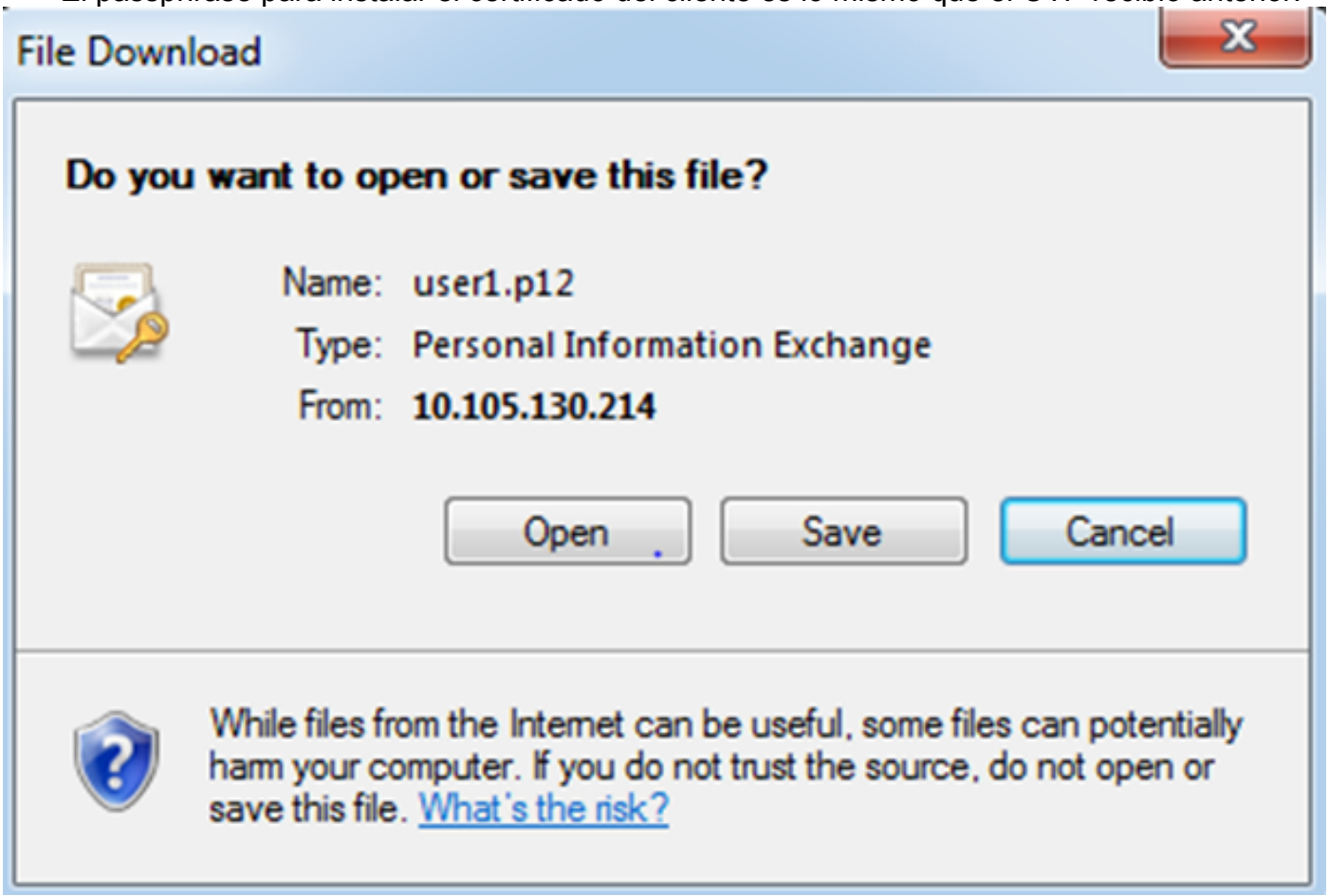
- En la estación de trabajo del cliente abra a un navegador y navegue al link para completar la inscripción.
- **El IP/FQDN** usado en este link debe ser el IP de la interfaz en la cual el **webvpn** se habilita en ese paso, que es **Internet de la interfaz**.

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

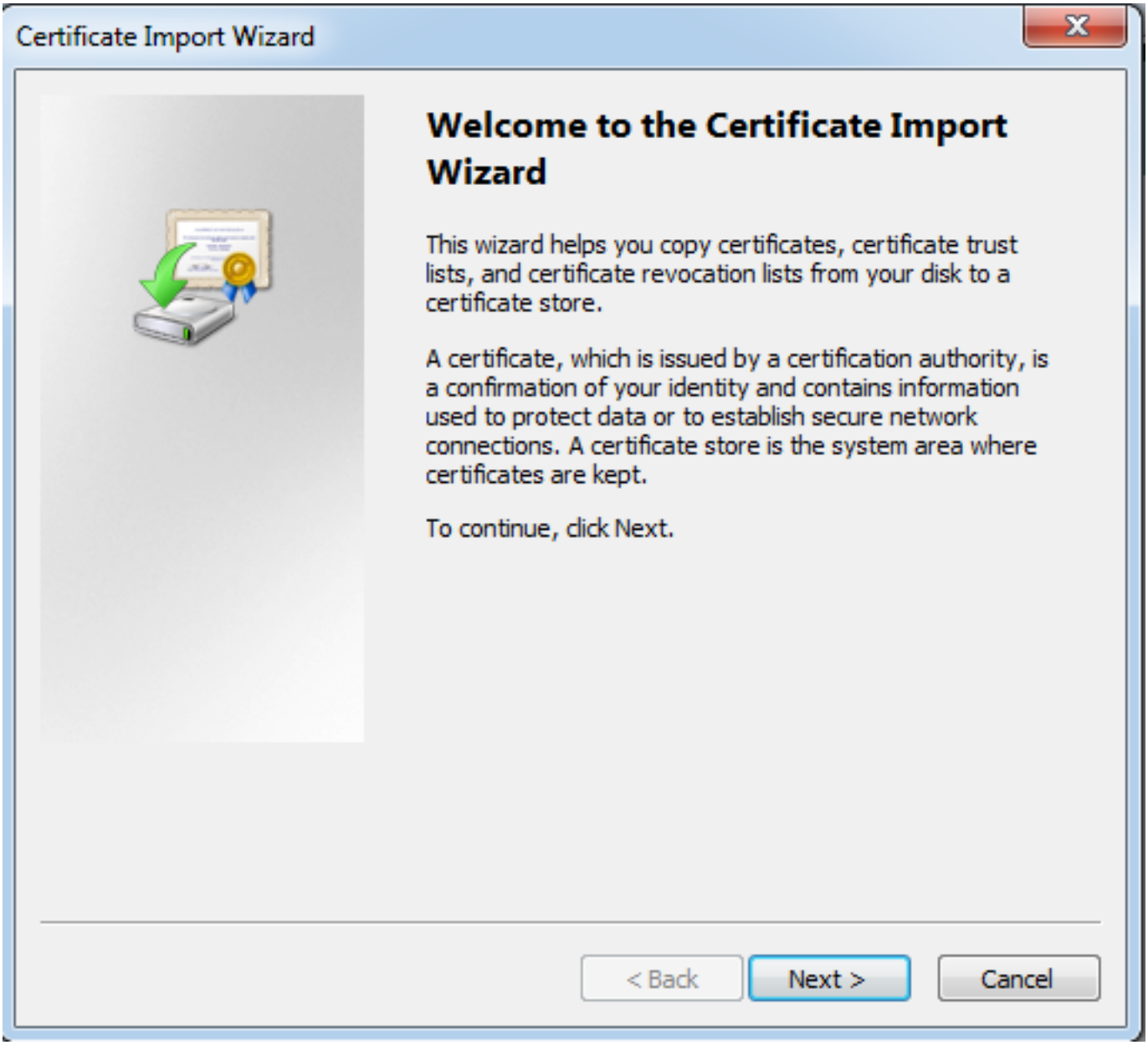
- Ingrese el nombre de usuario (configurado en el ASA bajo el paso 2, la opción A) y el **OTP,** que fue proporcionado vía el **email** o **manualmente**.



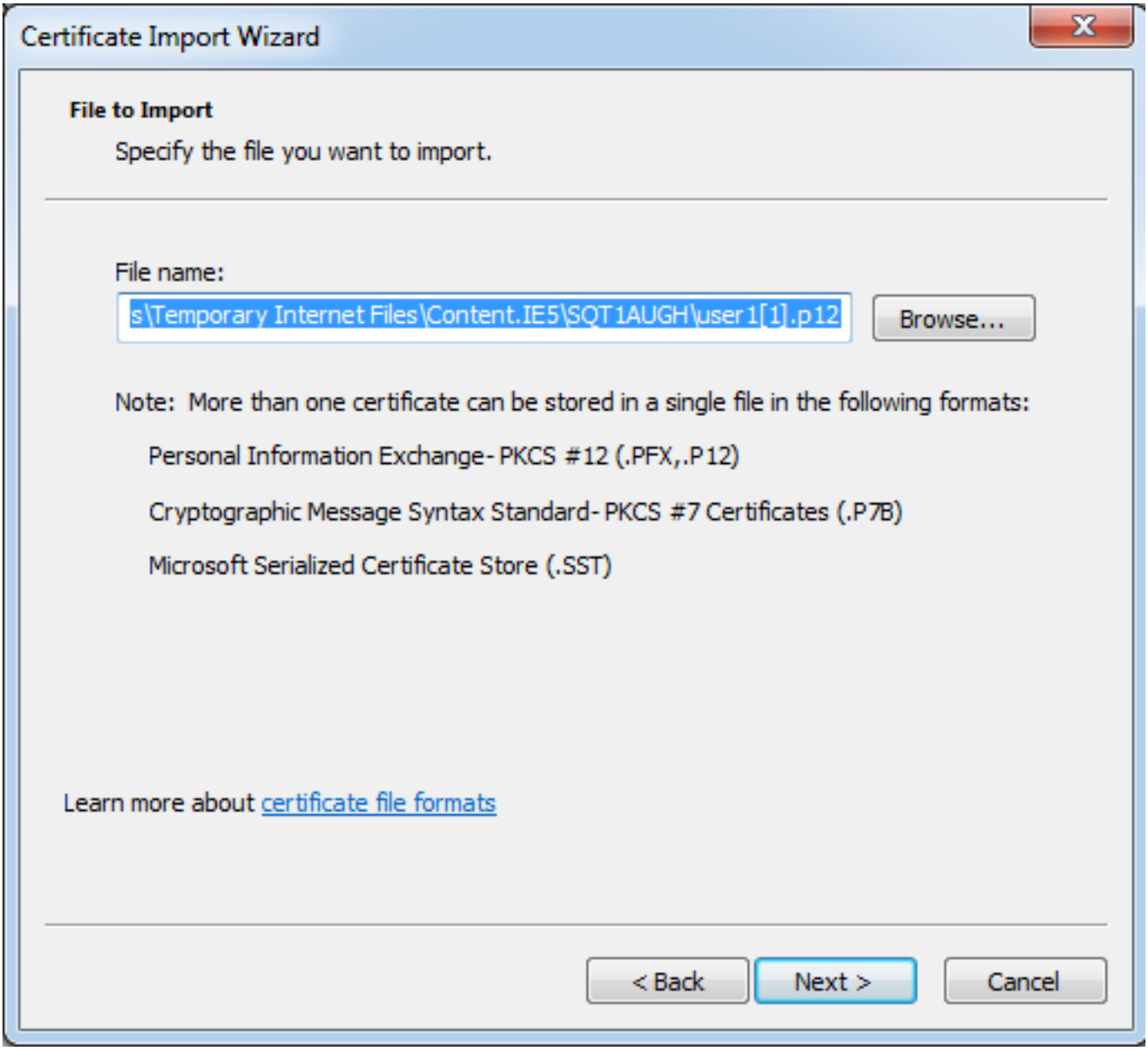
- Tecleo **abierto** instalar directamente el certificado del cliente recibido del ASA.
- El passphrase para instalar el certificado del cliente es lo mismo que el OTP recibió anterior.



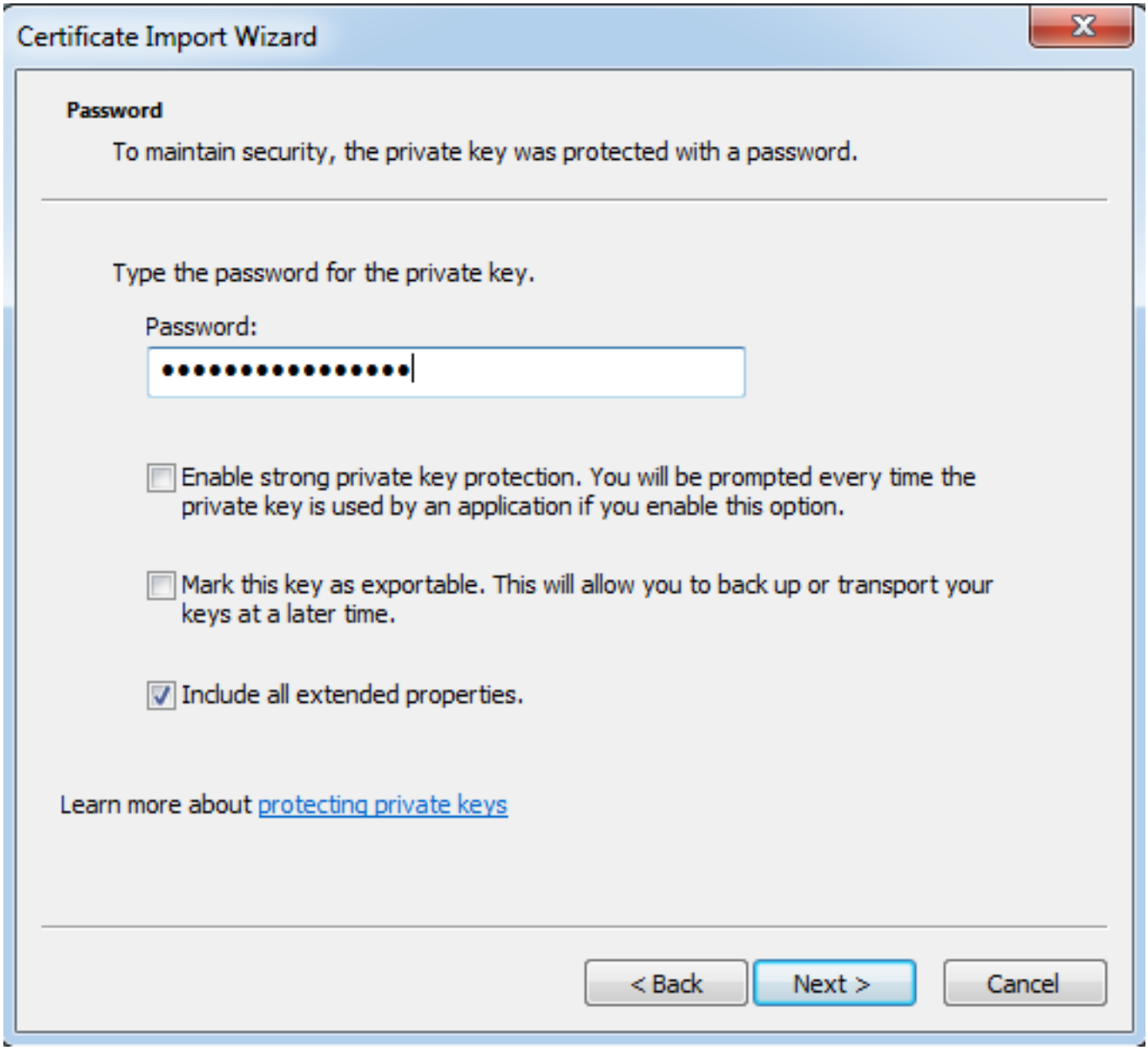
- Haga clic en Next (Siguiente).



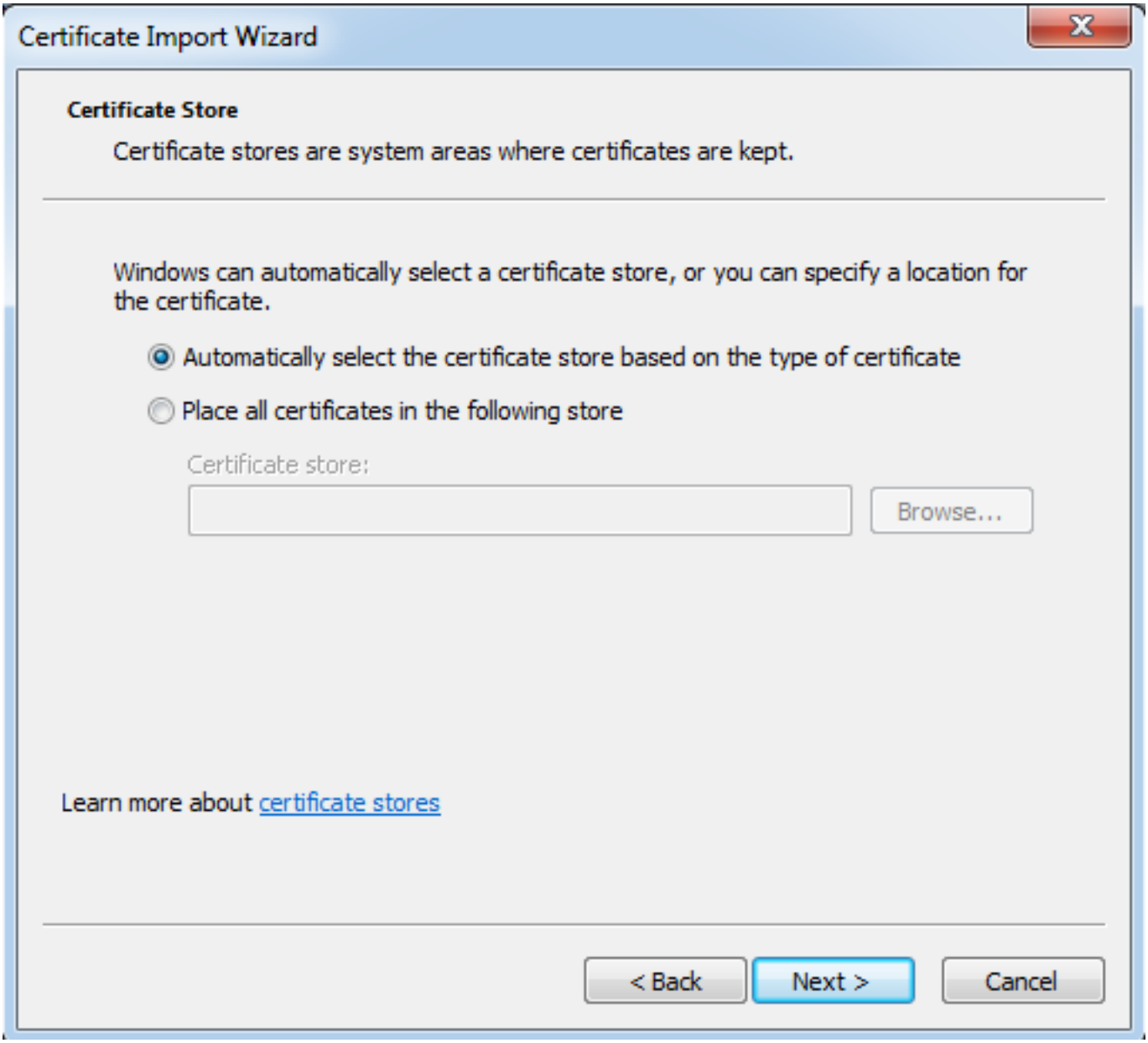
- Salga de la trayectoria como valor por defecto y haga clic **después**.



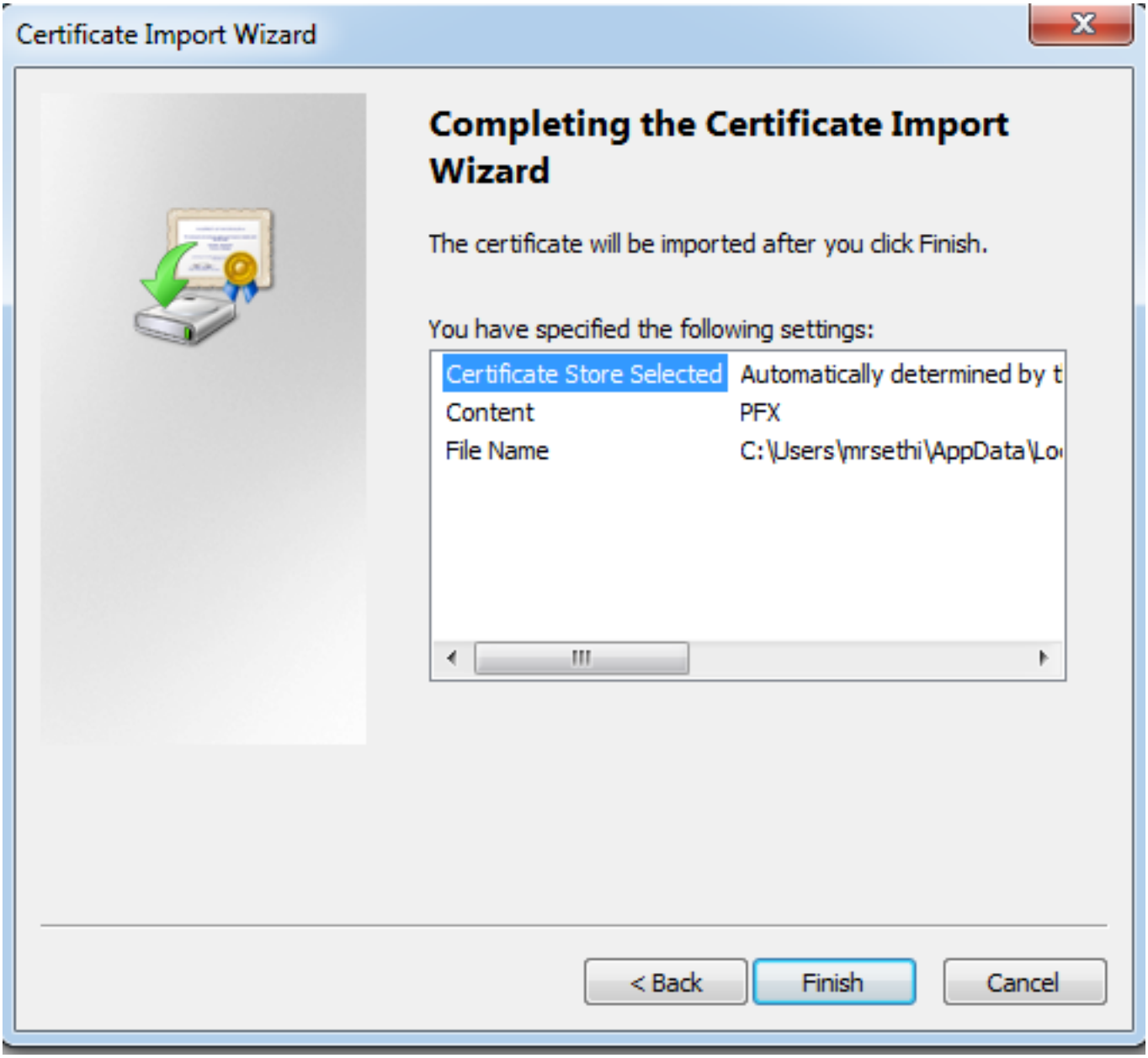
- Ingrese el OTP en el campo de contraseña.
- Usted puede seleccionar la opción **para marcar esta clave como exportable** de modo que la clave se pudiera exportar del puesto de trabajo en el futuro si procede.
- Tecleo **después**

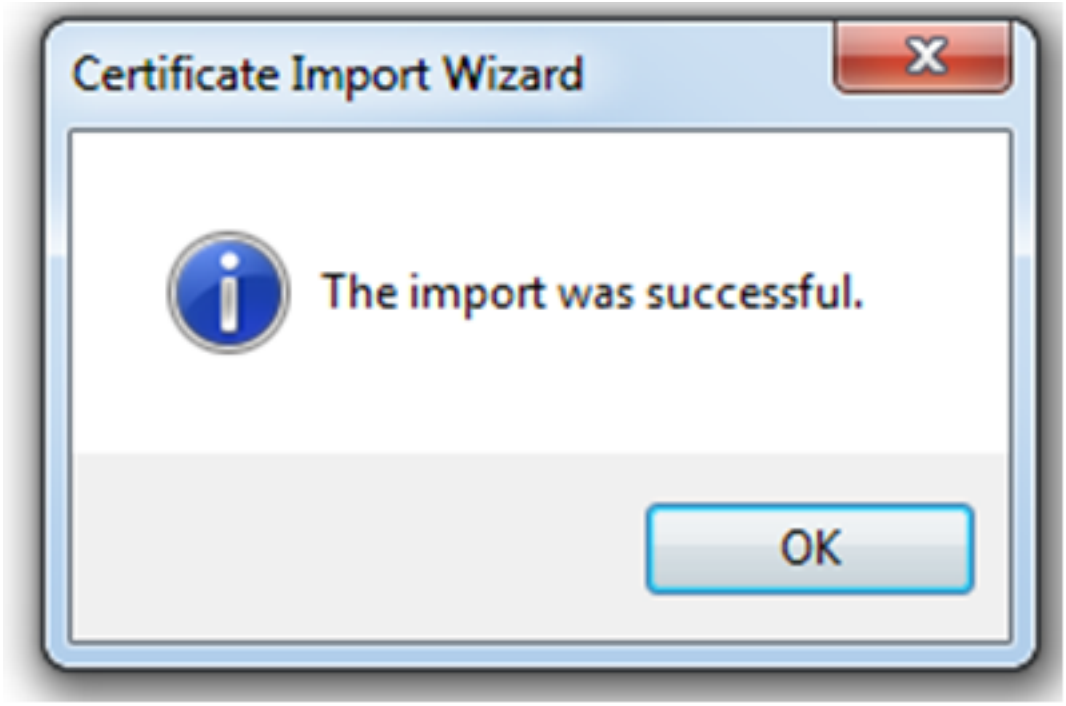


- Usted puede instalar manualmente el certificado en un almacén de certificados determinado o dejarlo para elegir automáticamente el almacén.
- Haga clic en Next (Siguiente).

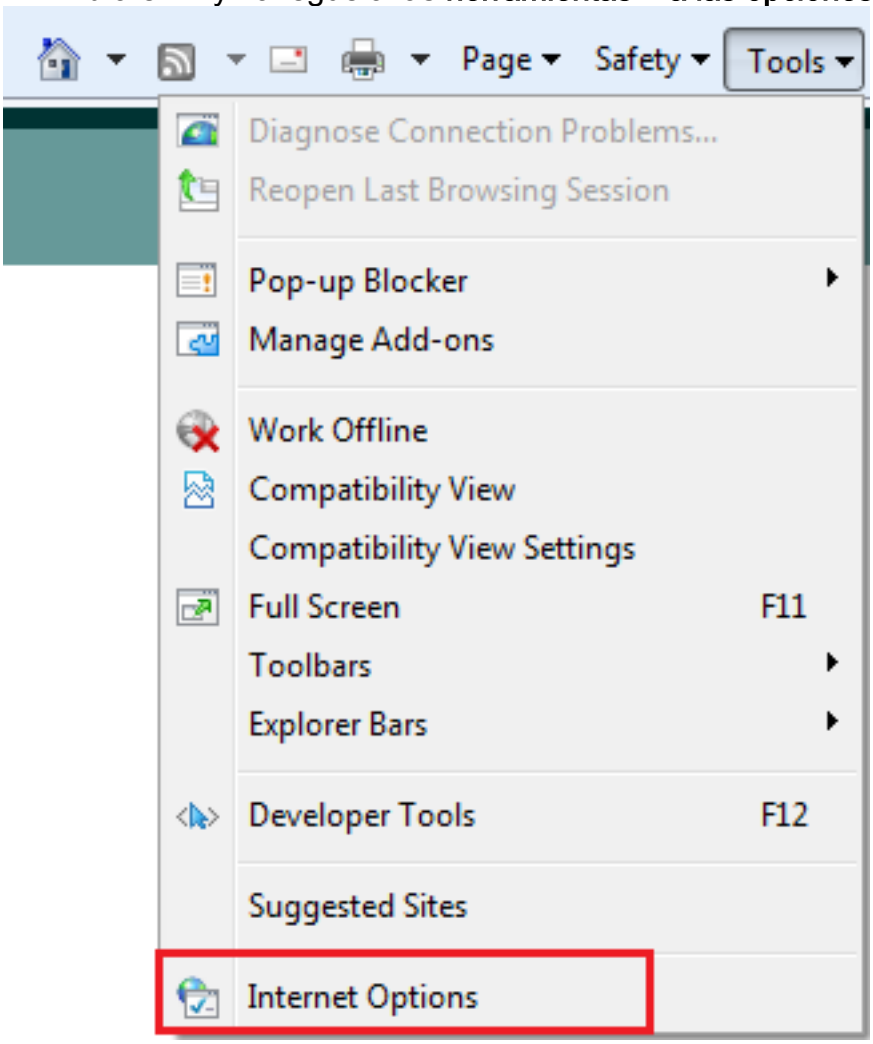


- Clic en Finalizar **para completar la instalación.**

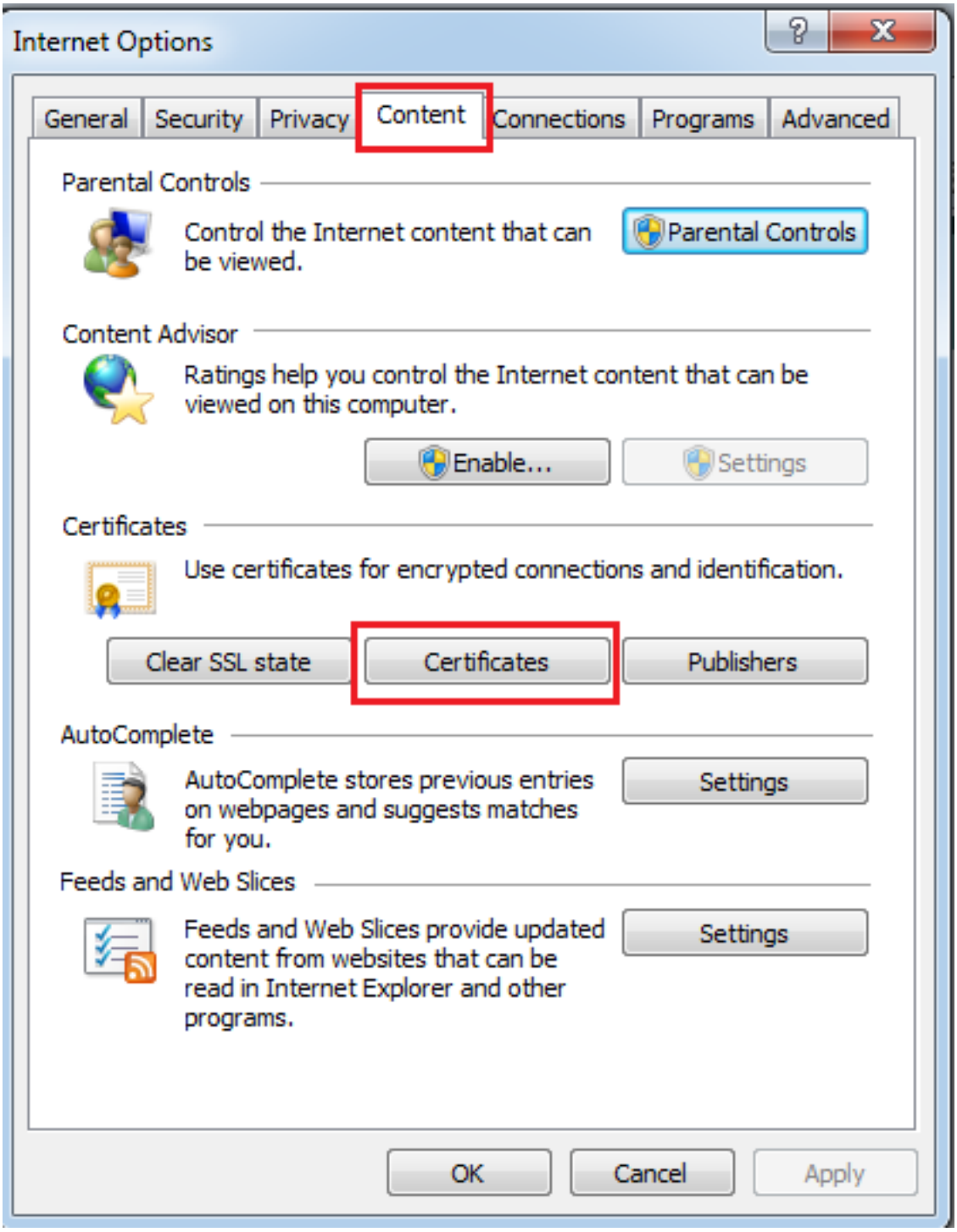

Certificate Import Wizard
Completing the Certificate Import Wizard
The certificate will be imported after you click Finish.
You have specified the following settings:
Certificate Store Selected
Automatically determined by t
Content
PFX
File Name
C:\Users\mrsethi\AppData\Lo
< Back
Finish
Cancel


Certificate Import Wizard
The import was successful.
OK

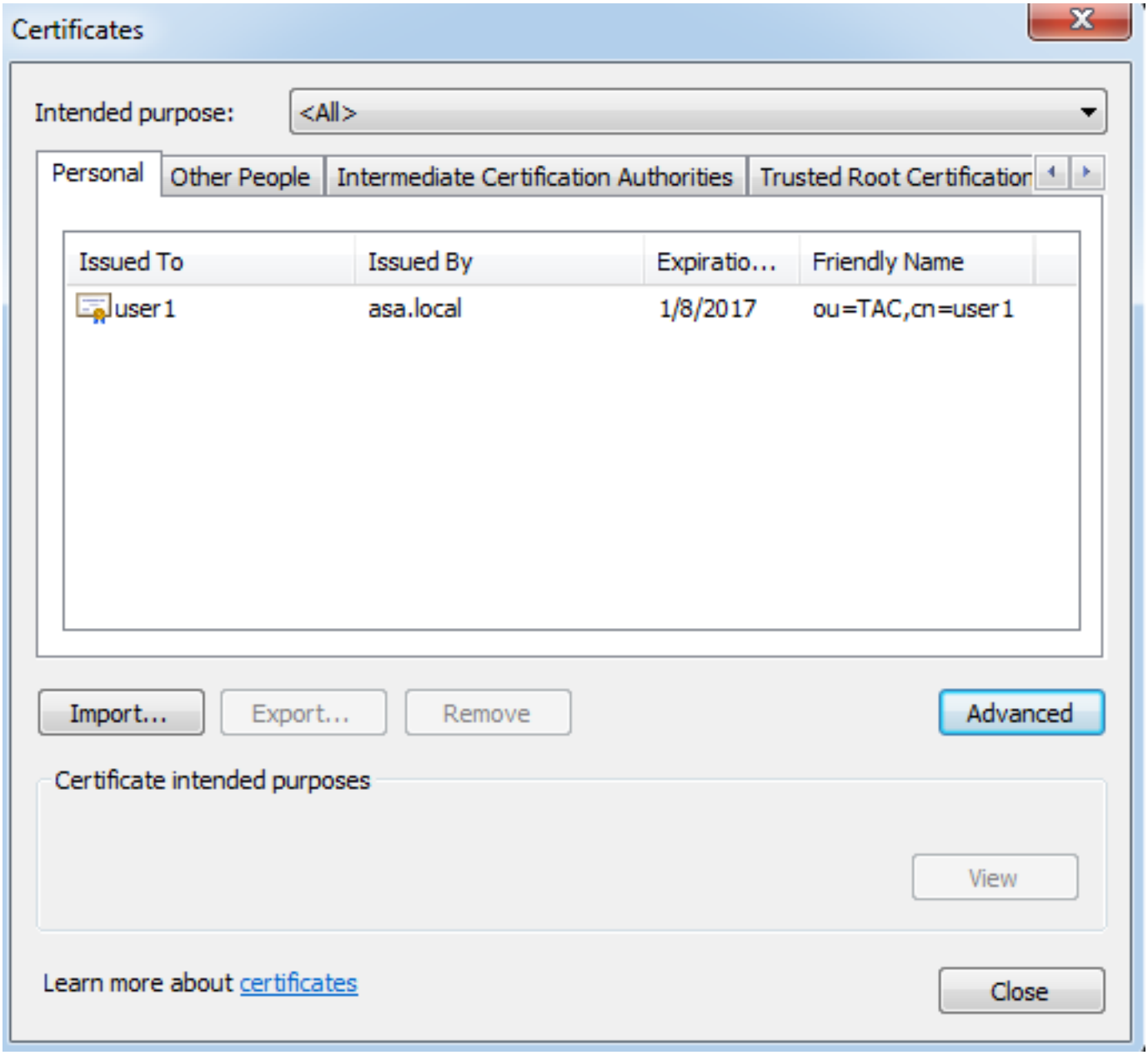
- Una vez que el certificado está instalado con éxito, usted puede verificarlo.
- Abra el IE y navegue a las **herramientas > a las opciones de Internet**.



- Navegue **para contentar la** lengueta y para hacer clic los **Certificados**, tal y como se muestra en de esta imagen.



- Bajo el almacén personal, usted puede ver el certificado recibido del ASA.



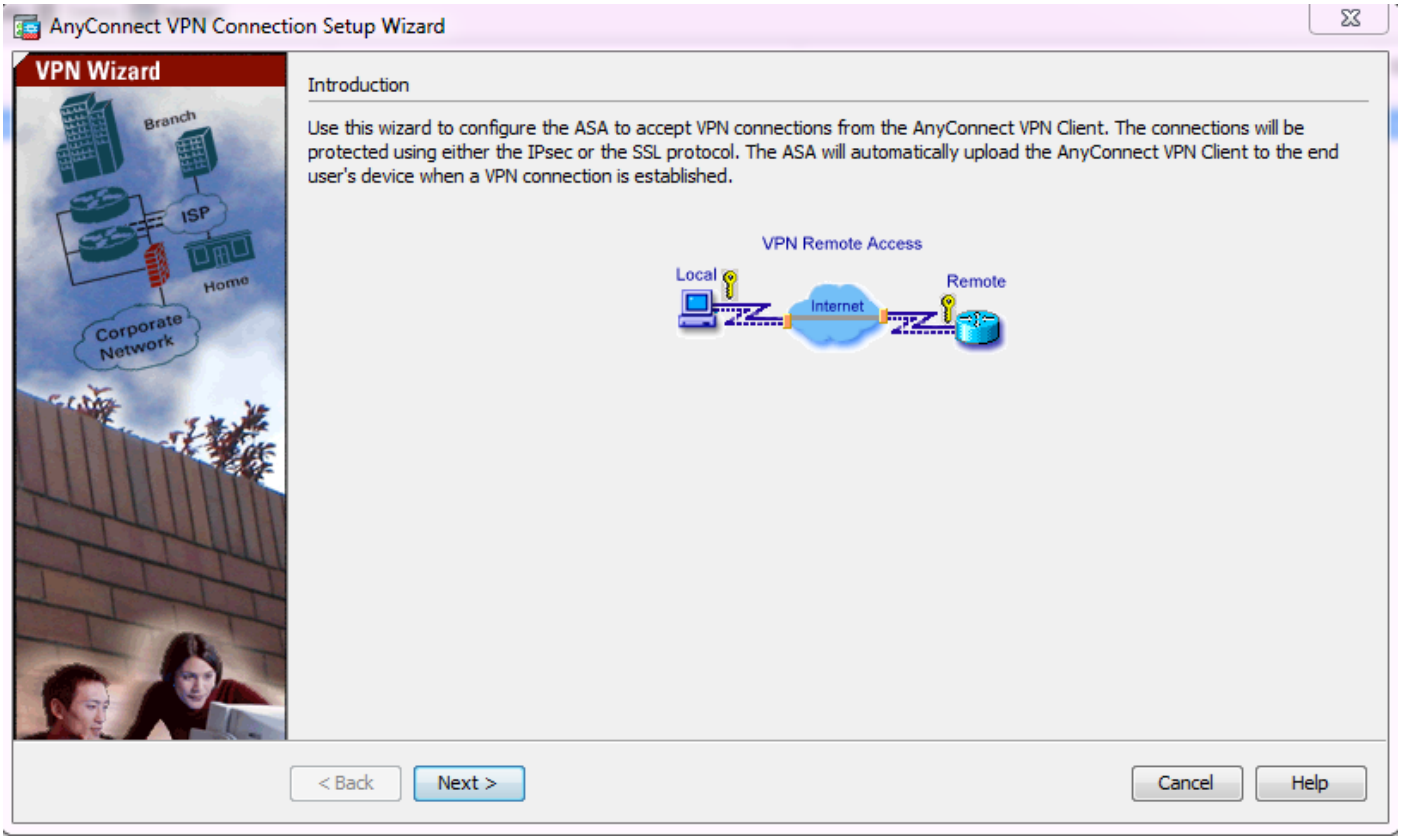
ASA como gateway SSL para los clientes de AnyConnect

Asistente de configuración de AnyConnect del ASDM

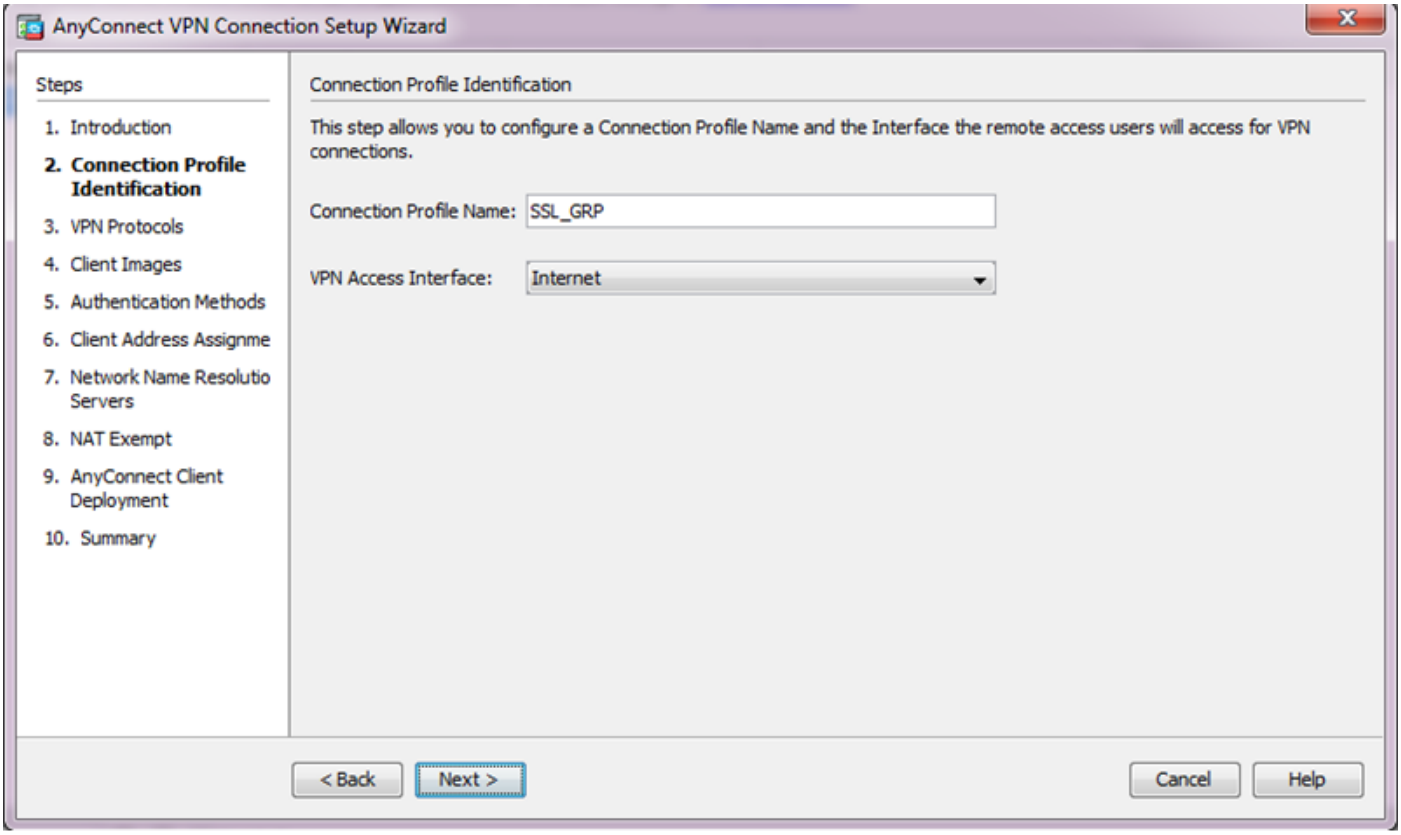
La configuración Wizard/CLI de AnyConnect se puede utilizar para configurar al cliente seguro de la movilidad de AnyConnect. Asegúrese de que un paquete del cliente de AnyConnect haya estado cargado al flash/al disco del Firewall ASA antes de que usted proceda.

Complete estos pasos para configurar al cliente seguro de la movilidad de AnyConnect vía el asistente de configuración:

1. El registro en el ASDM y navega a los **Asistentes VPN de Wizards> > al Asistente VPN de AnyConnect** para iniciar al asistente de configuración y a hacer clic **después**.

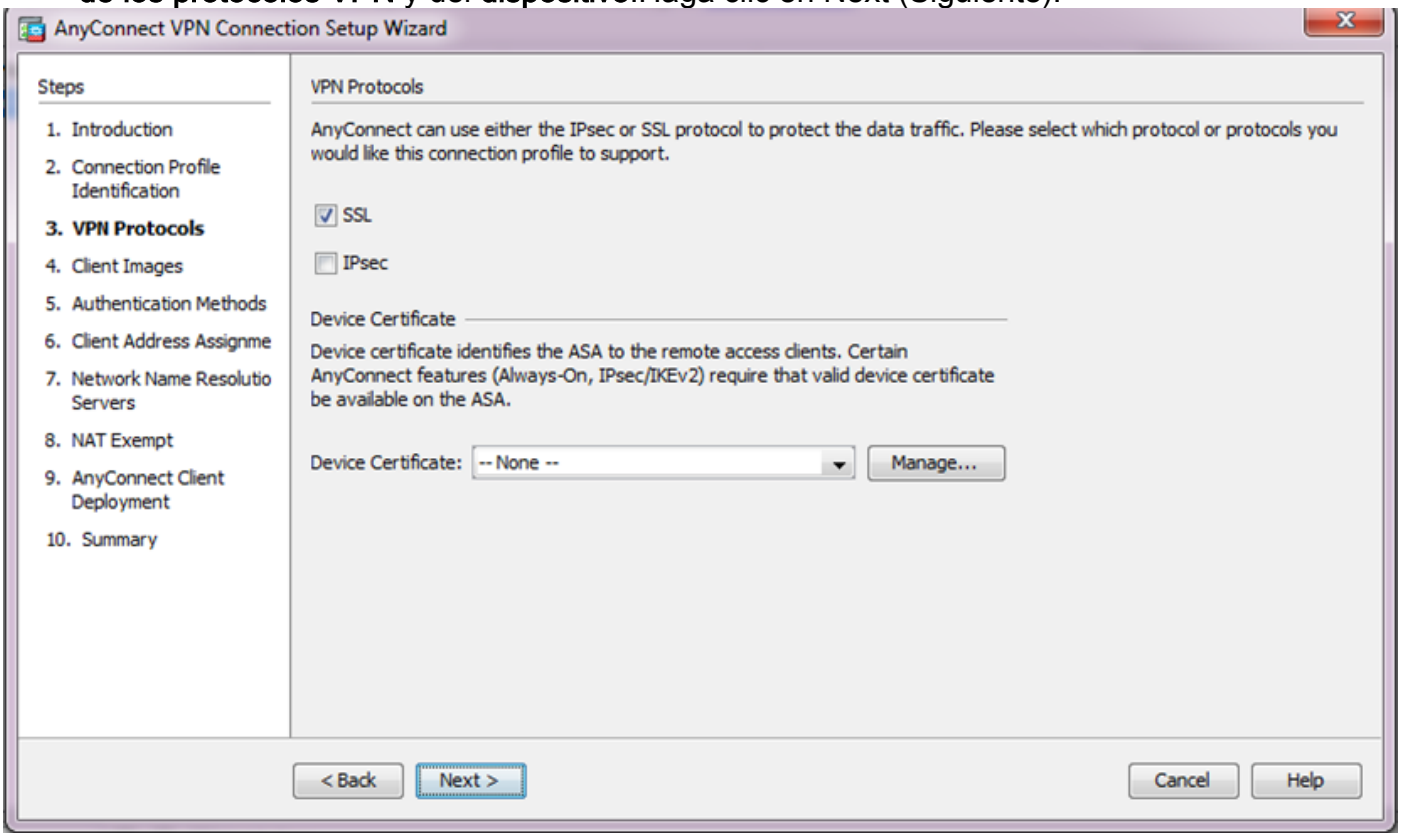


2. Ingrese el nombre del perfil de la conexión, elija la interfaz en la cual el VPN será terminado de la interfaz de acceso VPN el menú de persiana, y hace clic **después**.



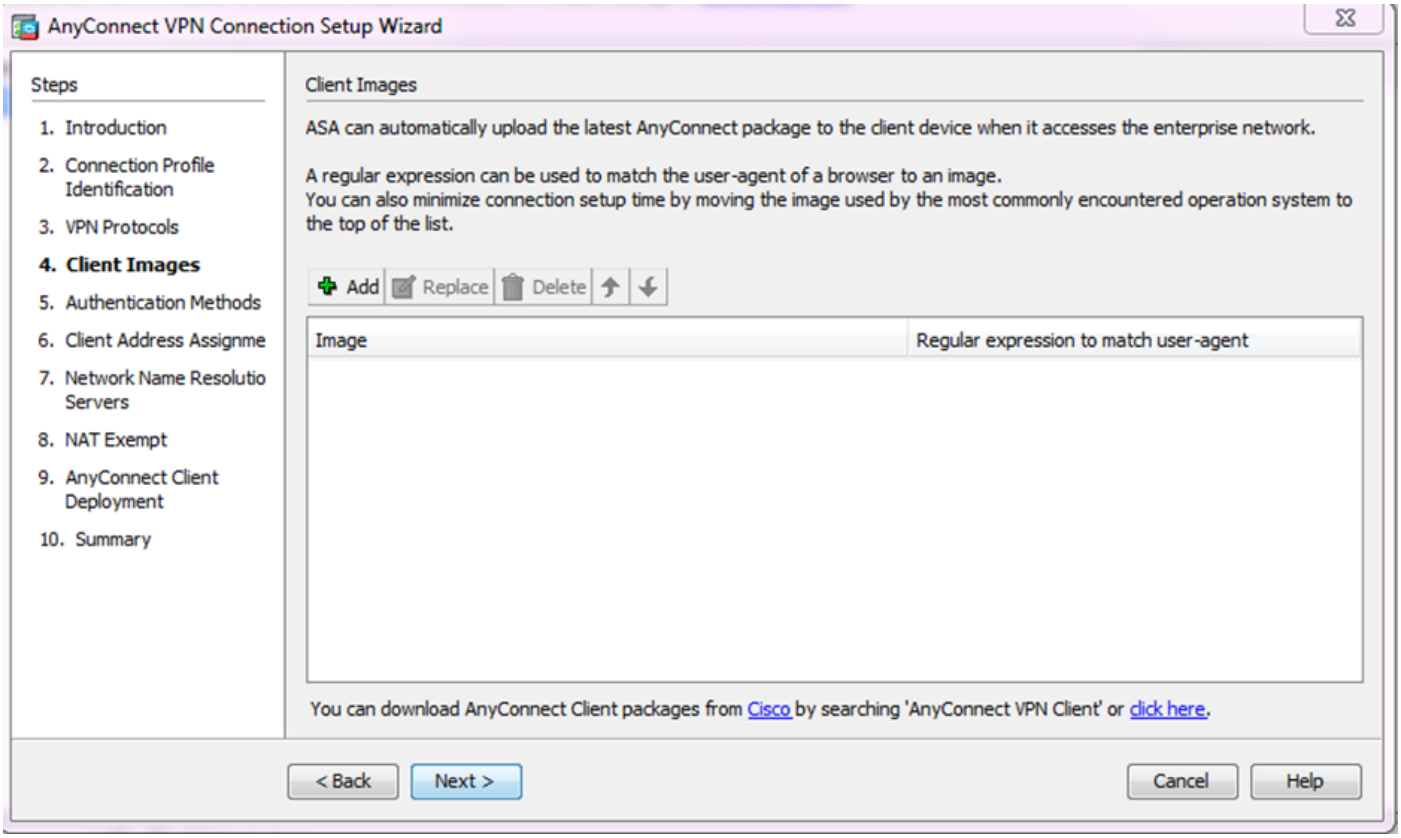
3. Marque la casilla de verificación **SSL** para habilitar Secure Sockets Layer (SSL). El certificado del dispositivo puede ser un certificado publicado Certificate Authority (CA) de confianza del otro vendedor (tal como Verisign, o confíe), o un certificado autofirmado. Si el certificado está instalado ya en el ASA, después puede ser elegido vía el menú desplegable.

1. **Note**: Este certificado es el certificado en el lado del servidor que será presentado por el ASA a los clientes SSL. Si no hay certificados de servidor instalados actualmente en el ASA que un certificado autofirmado debe ser generado, después haga clic **manejan**.Para instalar un certificado de tercera persona, complete los pasos que se describen en el ASA 8.x instalan manualmente los Certificados del vendedor de las de otras compañías para el uso con el documento de Cisco del ejemplo de configuración del WebVPN.Habilite el **certificado de los protocolos VPN** y del **dispositivo**.Haga clic en Next (Siguiente).

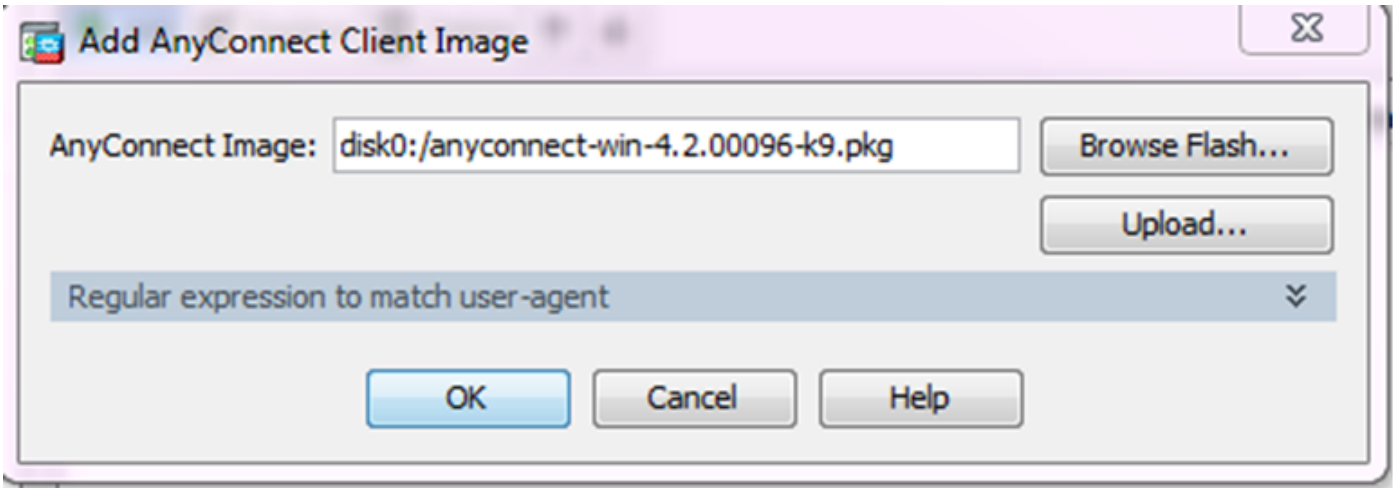


4. El tecleo **agrega** para agregar el paquete del cliente de AnyConnect (archivo .package) de la unidad local o del flash/del disco del ASA.

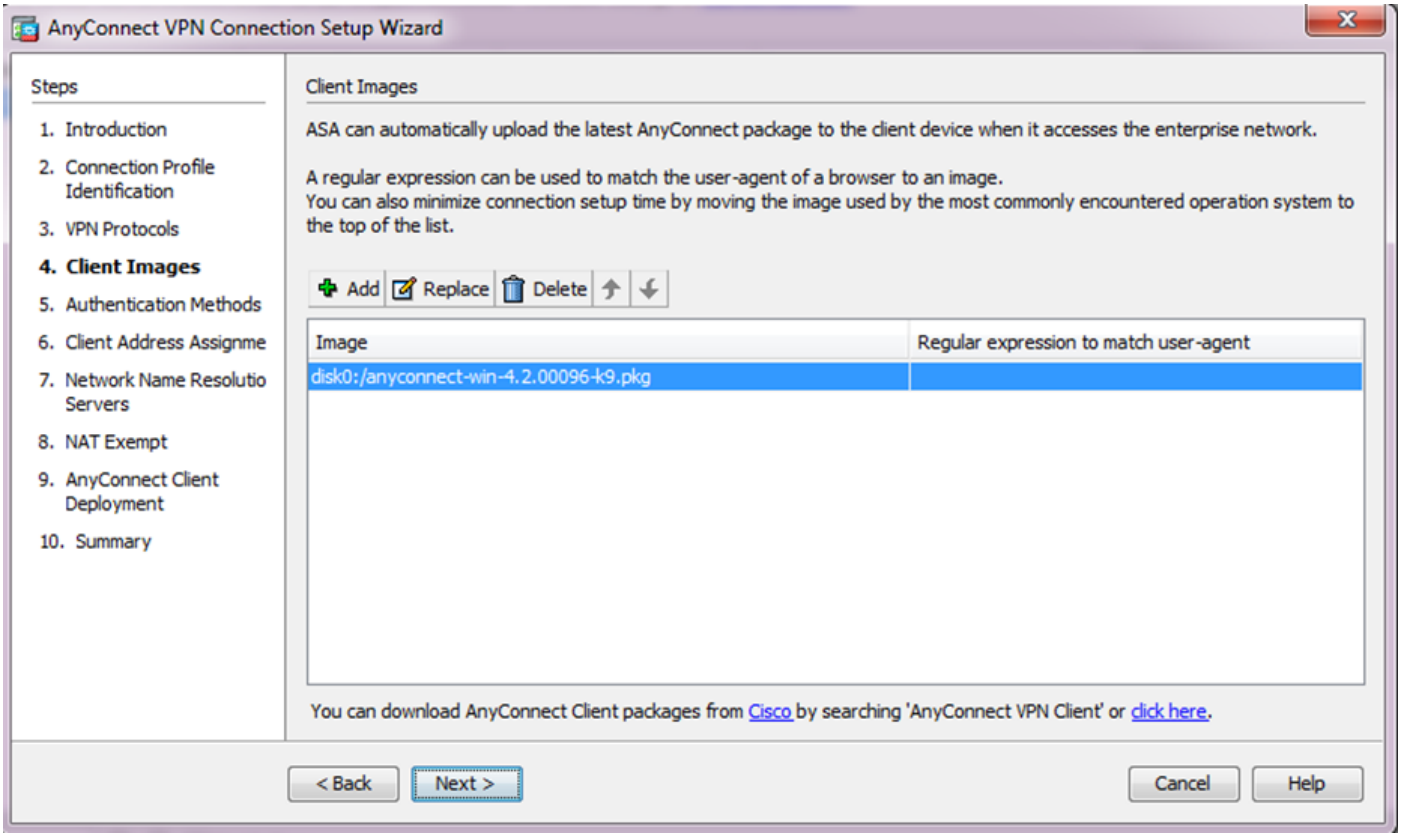
El tecleo **hojea el Flash** para agregar la imagen de memoria USB, o la **carga del** tecleo para agregar la imagen de la unidad local de equipo del host.



- Usted podría cargar el archivo AnyConnect.pkg cualquier del Flash/disco ASA (si el paquete está ya allí) o de la unidad local.
- Hojee el flash – para seleccionar el paquete de AnyConnect del Flash/disco ASA.
- Carga – seleccionar el paquete de AnyConnect de la unidad local de equipo del host.
- Click OK.

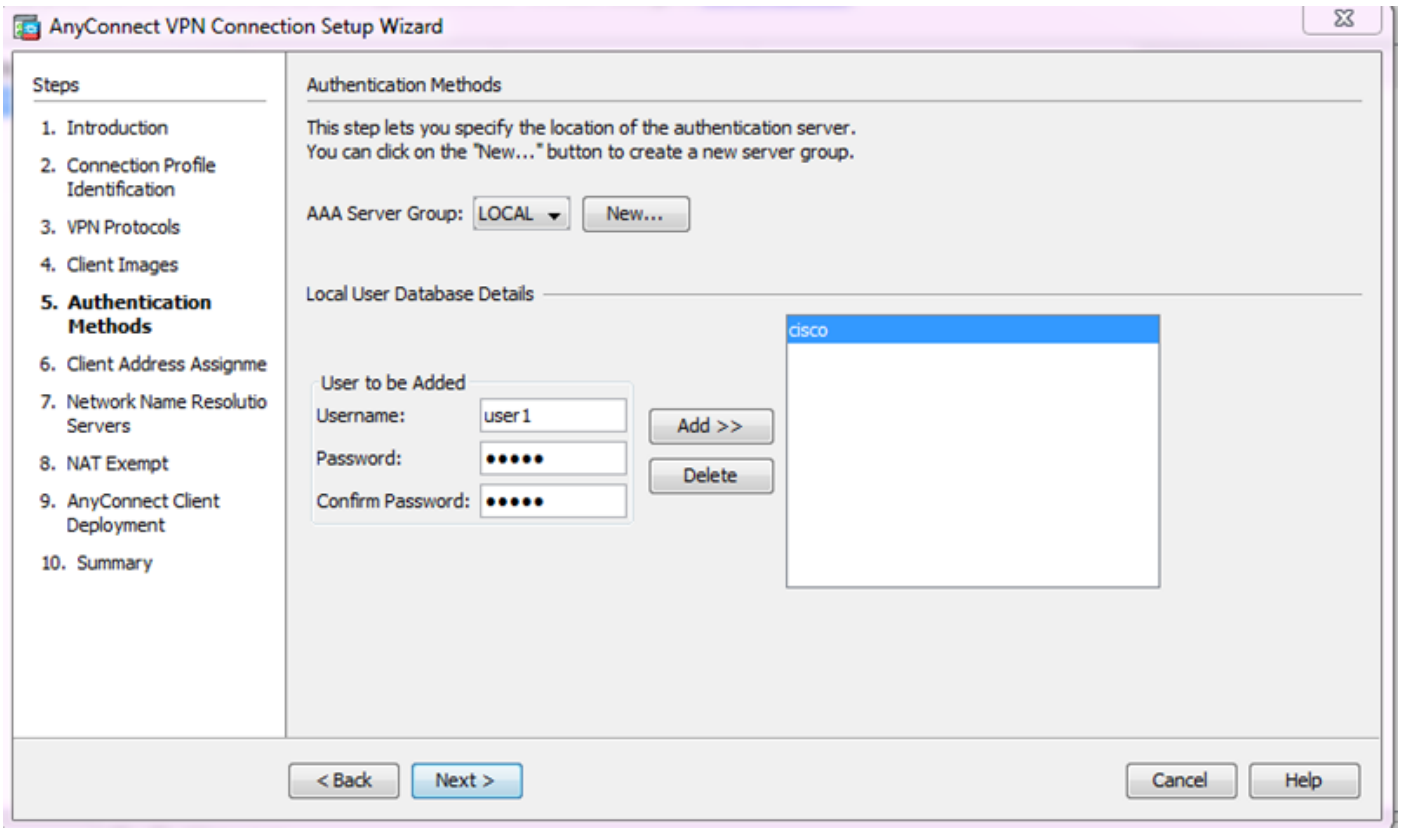


- Haga clic en Next (Siguiente).

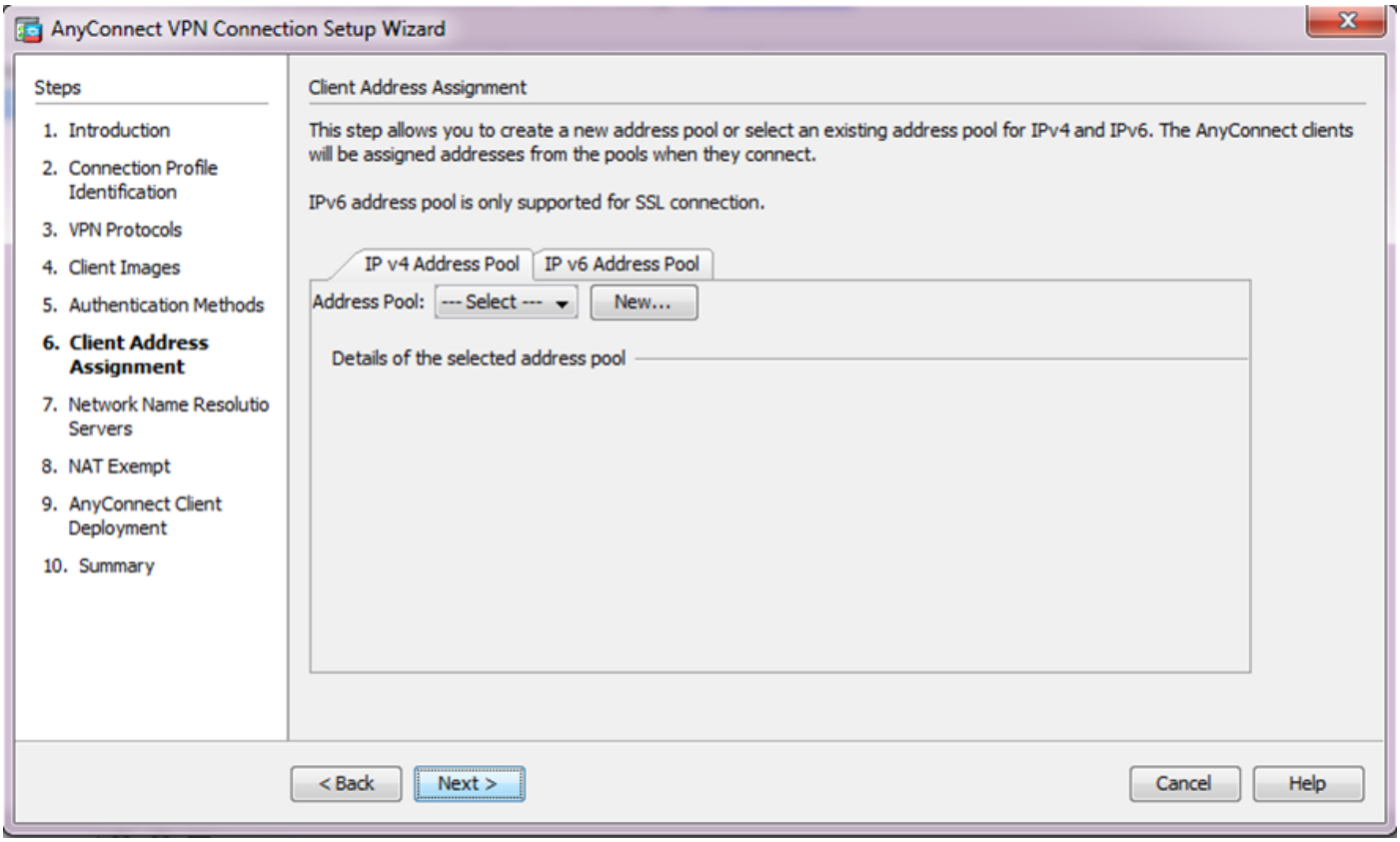


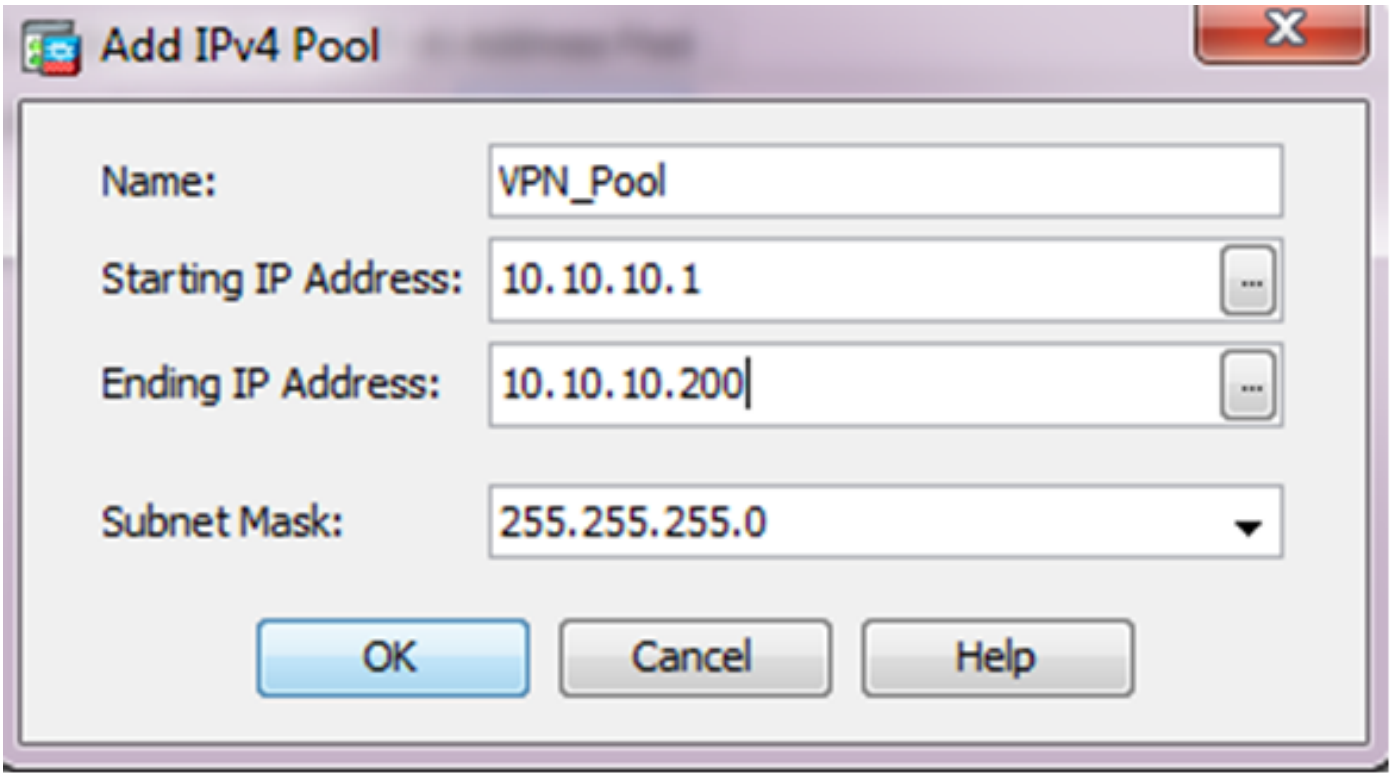
5. La autenticación de usuario se puede completar vía los grupos de servidores del Authentication, Authorization, and Accounting (AAA). Si configuran a los usuarios ya, después elija el **LOCAL** y haga clic **después**. Agregue a un usuario a la base de datos de usuarios locales y haga clic **después**.

> **Note**: En este ejemplo, se configura la **autenticación local**, así que significa que la base de datos de usuarios locales en el ASA será utilizada para la autenticación.

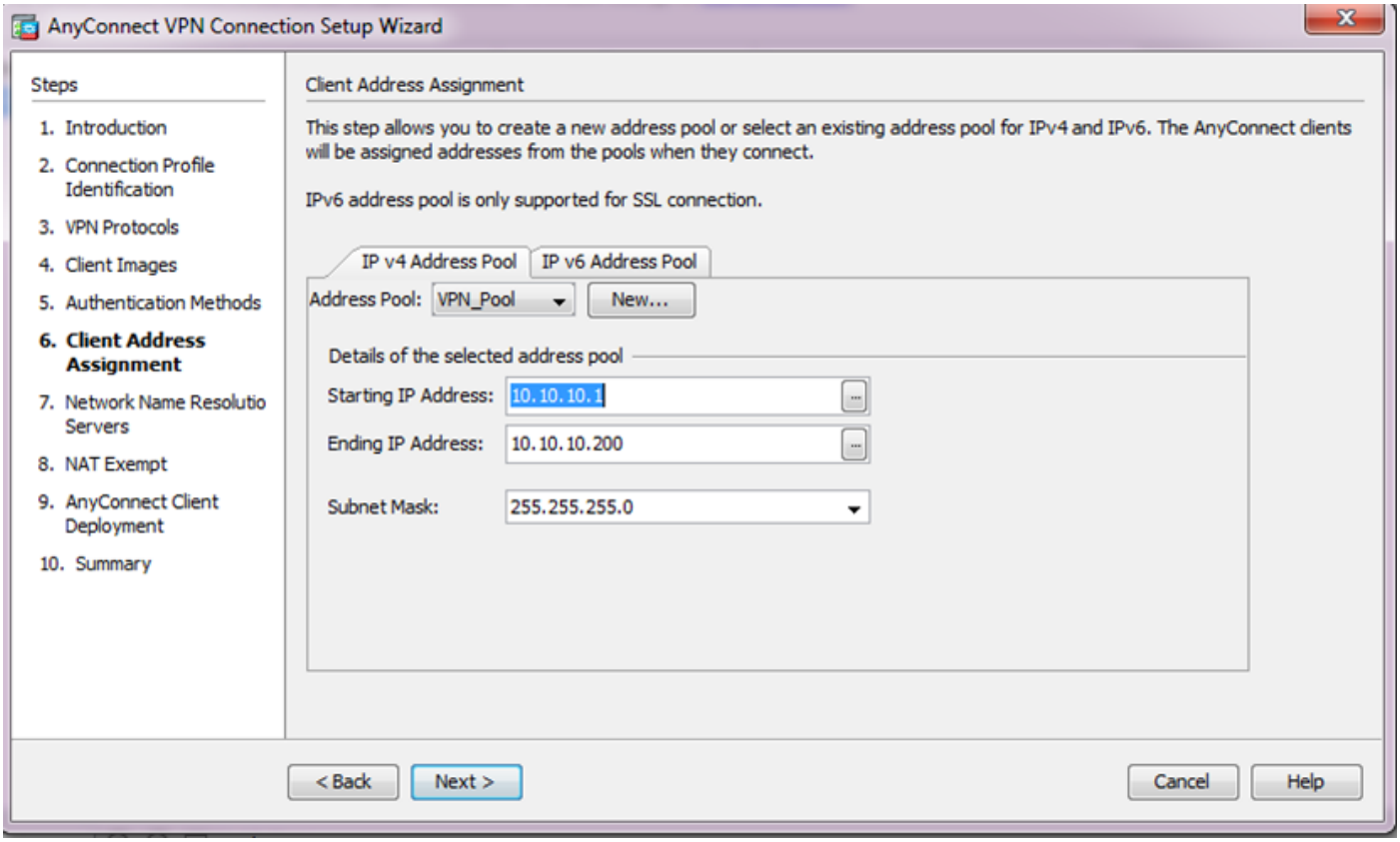


6. Asegúrese de que configuren a la agrupación de direcciones para los clientes VPN. Si un pool del IP entonces se configura ya selecciónelo del menú desplegable. Si no, haga clic **nuevo** para configurar. Complete, haga clic una vez **después**.

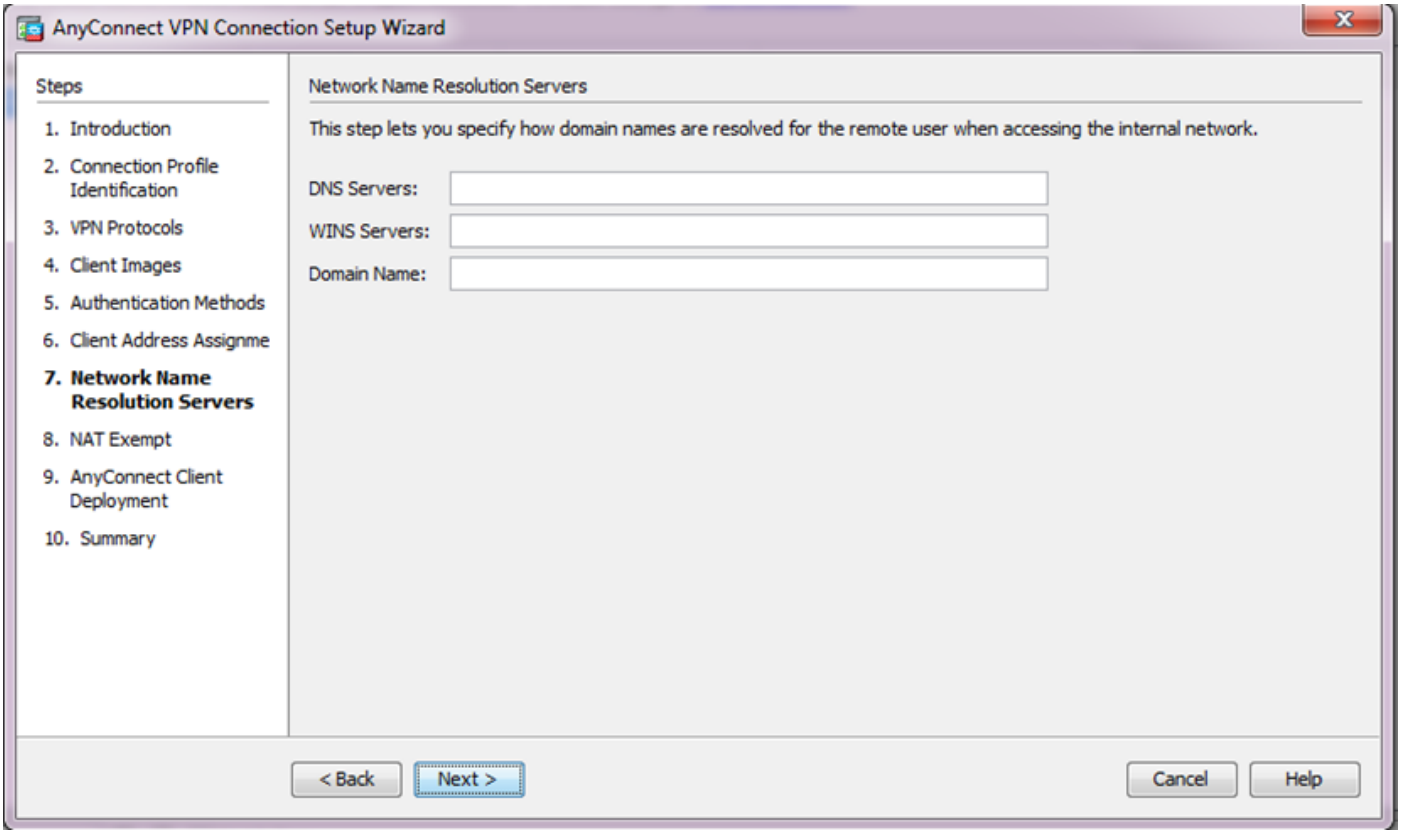




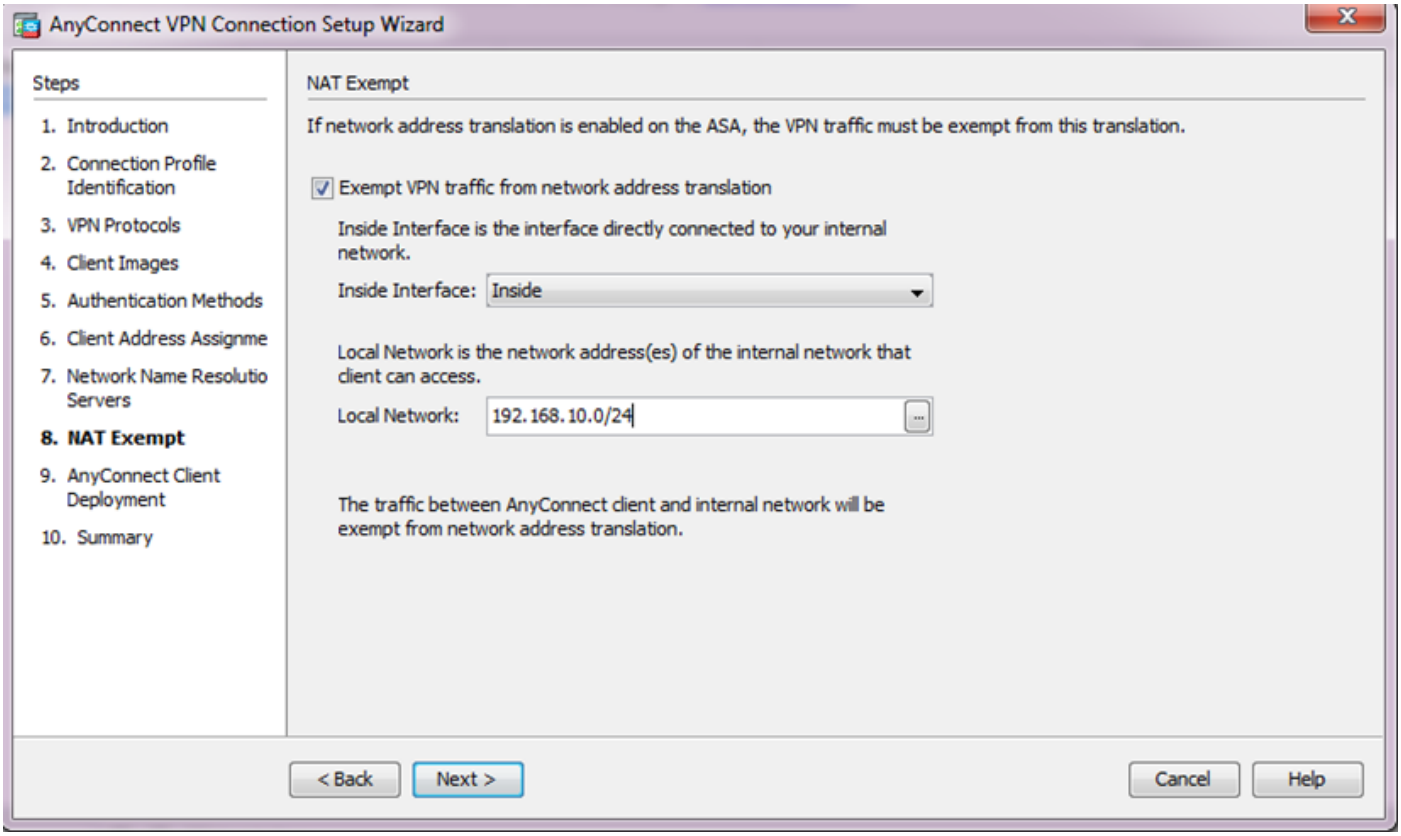
- Haga clic en Next (Siguiente).



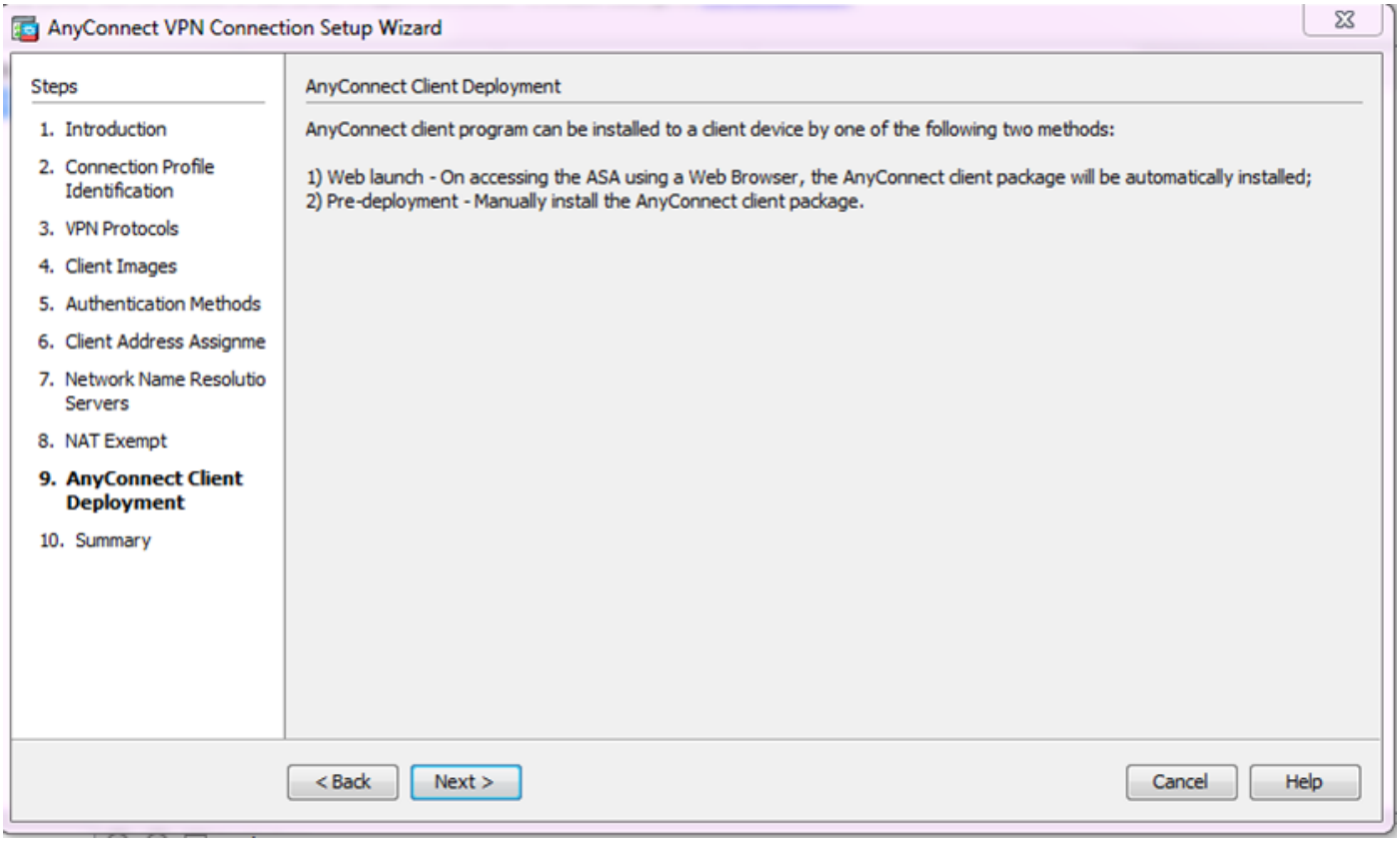
7. Opcionalmente, configure los servidores del Domain Name System (DNS) y los DN en los campos DNS y del Domain Name, y después haga clic **después**.



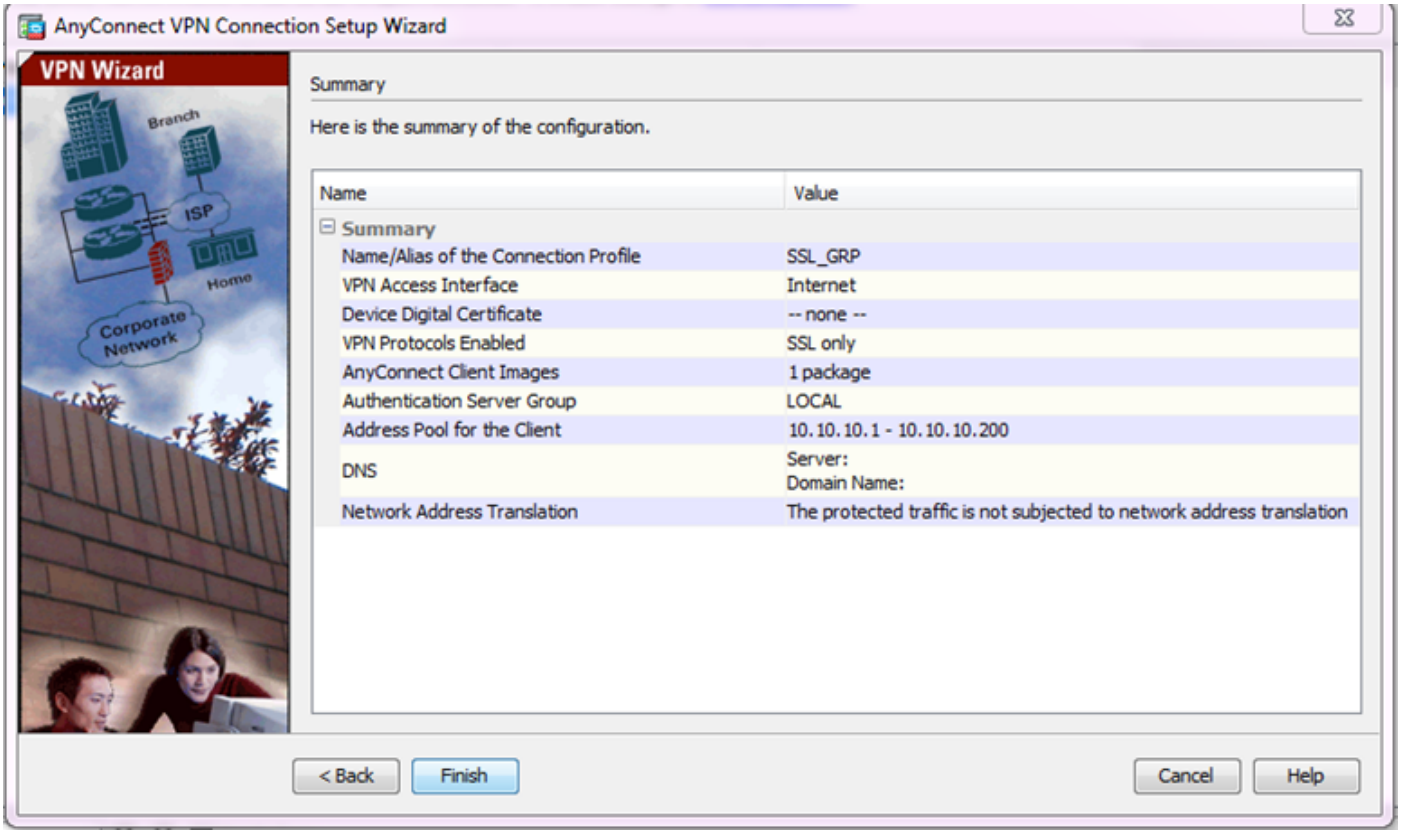
8. Asegúrese de que el tráfico entre el cliente y la subred interior deba estar exento de cualquier traducción de dirección de red dinámica (NAT). Habilite el **tráfico exento VPN de la** casilla de verificación de la **traducción de dirección de red** y configure la interfaz LAN que será utilizada para la exención. También, especifique la red local que se debe eximir y tecleo **después**.



9. Haga clic en Next (Siguiente).

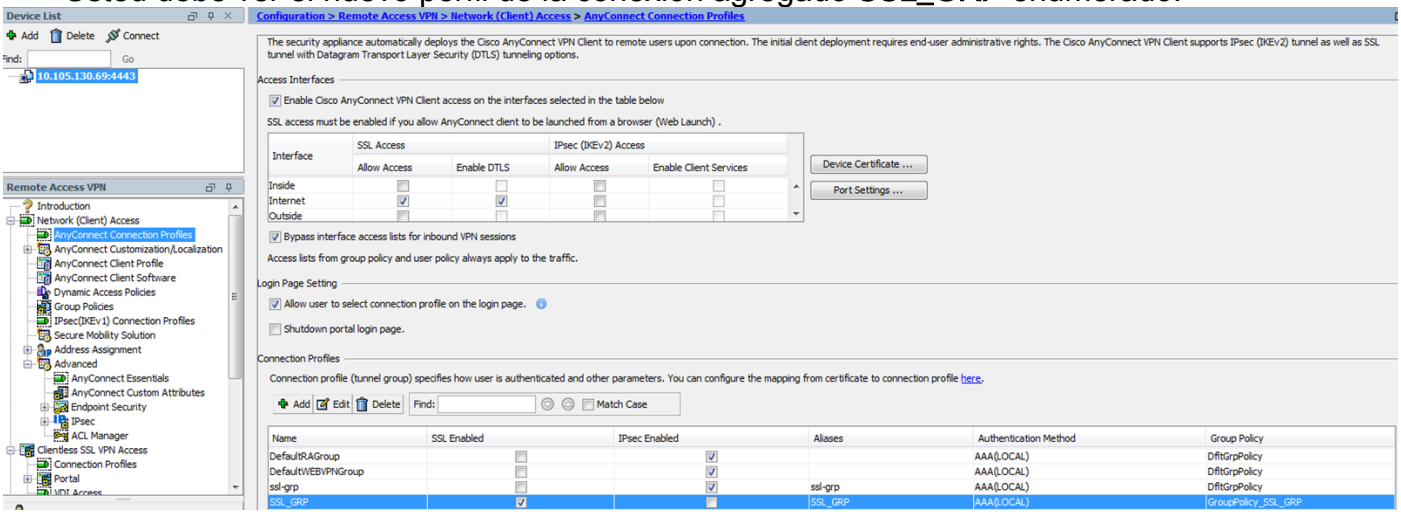


10. El último paso muestra el resumen, clic en Finalizar para completar la configuración.

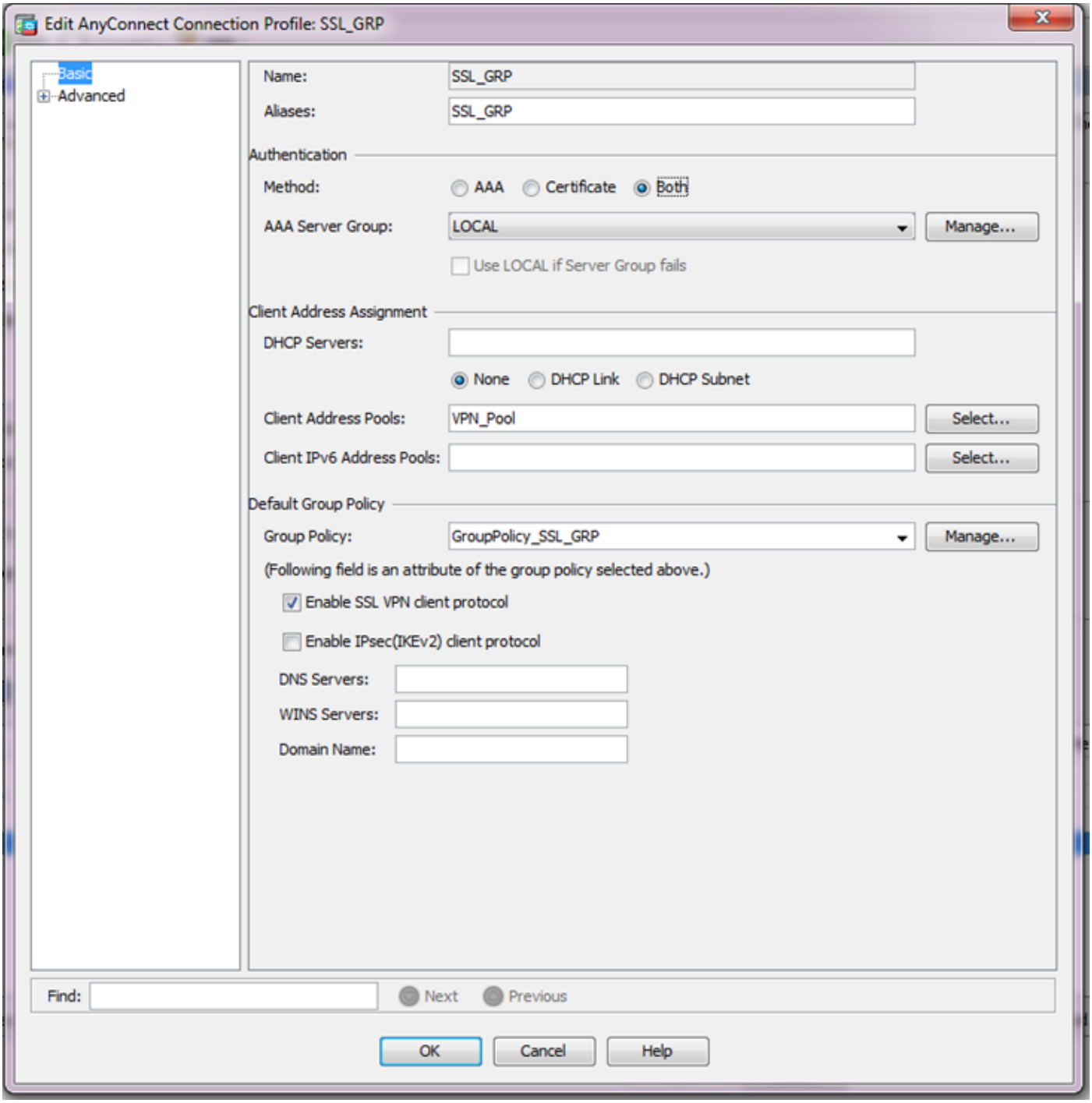


La configuración del cliente de AnyConnect es completa ahora. Sin embargo, cuando usted configura AnyConnect vía el asistente de configuración, configura el **método de autentificación como AAA** por abandono. Para autenticar a los clientes vía los Certificados y el nombre de usuario/la contraseña, el grupo de túnel (perfil de la conexión) se debe configurar para utilizar los Certificados y el AAA como el método de autentificación.

- Navegue a la **configuración > al acceso del VPN de acceso remoto > de la red (cliente) > a los perfiles de la conexión de AnyConnect**.
- Usted debe ver el nuevo perfil de la conexión agregado **SSL_GRP** enumerado.



- Para configurar el **AAA** y la **autenticación certificada**, seleccionar el perfil de la conexión **SSL_GRP** y el tecleo **edite**.
- Bajo método de autentificación, seleccione **ambos**.



Configure el 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 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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

> **Note**: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Asegúrese de que el servidor de CA esté habilitado.

muestre el servidor crypto 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!!
```

Asegúrese de que se permita al usuario para la inscripción después de agregar:

```
*****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
```

Usted puede marcar los detalles de la conexión del anyconnect vía el CLI o el ASDM.

Vía el CLI

muestre el anyconnect del detalle de 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 :
```

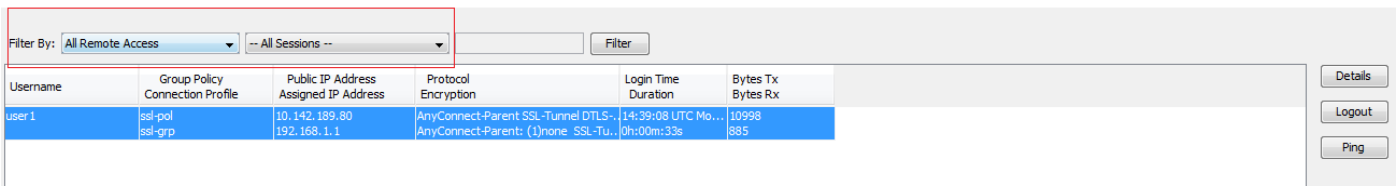
Vía el ASDM

- Navegue a **monitorear > VPN > los VPN statistics (Estadísticas de la VPN) > las sesiones**.
- Elija el **filtro por** como **todo el Acceso Remoto**.
- Usted puede realizar cualquiera de las acciones para el cliente seleccionado de AnyConnect.

Los detalles proporcionan más información sobre la sesión

Fin de comunicación para terminar sesión manualmente al usuario del headend

Haga ping para hacer ping al cliente de AnyConnect del headend



Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su

configuración.

> **Note**: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

> **Caution**: En el ASA, usted puede fijar los diversos niveles de debug; por abandono, se utiliza el nivel 1. Si usted cambia el nivel de debug, la verbosidad de los debugs pudo aumentar. Haga esto con cautela, especialmente en los entornos de producción.

- **debug crypto ca**
- **servidor del debug crypto ca**
- **mensajes del debug crypto ca**
- **transacciones del debug crypto ca**
- **anyconnect del webvpn del debug**

Esta salida de los debugs muestra cuando el servidor de CA se habilita usando el **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!
```

Esta salida de los debugs muestra la inscripción del cliente

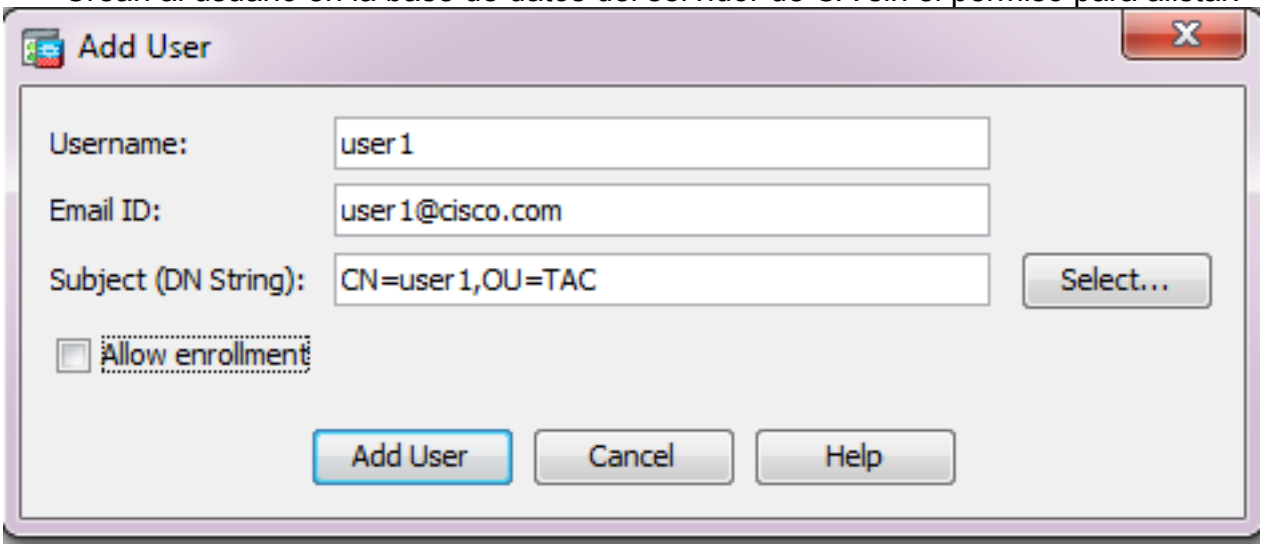
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255

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
```

La inscripción del cliente puede fallar bajo estas condiciones:

Escenario 1.

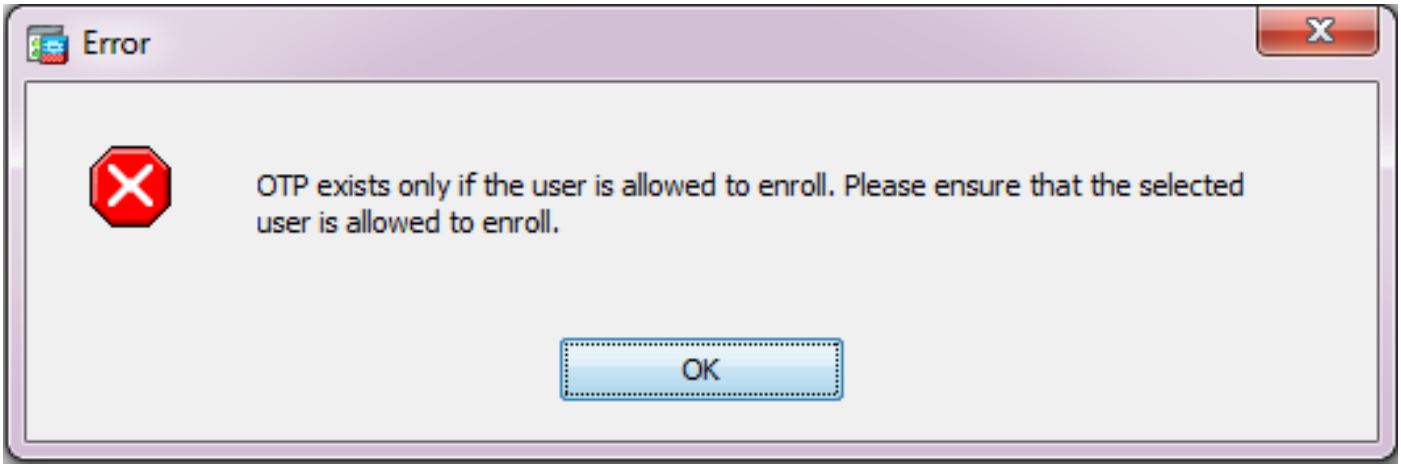
- Crean al usuario en la base de datos del servidor de CA sin el permiso para alistar.



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
```

- En el caso donde no se permite al usuario alistar, intentando generar/correo electrónico el OTP para el usuario genera este mensaje de error.



Escenario 2.

- Verifique el puerto e interconecte en cuál está disponible el portal de la inscripción con el **comando webvpn del funcionamiento de la demostración**. **El puerto predeterminado es 443** pero puede ser modificado.

- Asegúrese de que el cliente tenga alcance de la red a la **dirección IP de la interfaz** en la cual el **webvpn** se habilita en el puerto usado para acceder con éxito el portal de la inscripción.

El cliente puede no poder acceder el portal de la inscripción del ASA en estos casos:

1. Si cualquier dispositivo intermedio bloquea las conexiones entrantes del cliente al IP del **webvpn del** ASA en el puerto especificadas.
2. El estado de la interfaz está abajo en se habilita qué **webvpn**.

- Esta salida muestra que el portal de la inscripción está disponible en la **dirección IP de Internet de la interfaz** en el **puerto** de encargo **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
```

Escenario 3.

- La ubicación predeterminada del almacenamiento de la base de datos del servidor de CA es memoria flash del ASA.
- Asegúrese de que memoria flash tenga espacio libre para generar y para salvar el archivo del **pkcs12** para el usuario durante la inscripción.
- En el caso donde memoria flash no tiene bastante espacio libre, el ASA no puede completar el proceso de la inscripción del cliente y genera estos registros del debug:

```
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
```

Información Relacionada

- Cisco ASA 5500 Series Adaptive Security Appliances
- Guía de Troubleshooting del cliente VPN de AnyConnect - Problemas comunes
- Manejando, monitoreando, y resolver problemas las sesiones de AnyConnect
- Soporte Técnico y Documentación - Cisco Systems