Configurazione di ASA come server CA locale e headend AnyConnect

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) come server CA (Certification Authority) e come gateway SSL (Secure Sockets Layer) per i client Cisco AnyConnect Secure Mobility.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione ASA di base con software versione 9.1.x
- ASDM 7.3 o versione successiva

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco serie 5500 ASA con software versione 9.1(6)
- AnyConnect Secure Mobility Client versione 4.x per Windows
- PC che esegue un sistema operativo supportato in base alla tabella di compatibilità.
- Cisco Adaptive Security Device Manager (ASDM) versione 7.3

> Nota: scaricare il pacchetto AnyConnect VPN Client (anyconnect-win*.pkg) da Cisco Software Download (solo utenti registrati). Copiare il client VPN AnyConnect nella memoria flash dell'ASA, da scaricare sui computer degli utenti remoti per stabilire la connessione VPN SSL con l'ASA. Per ulteriori informazioni, consultare la sezione Installazione del client AnyConnect della guida alla configurazione delle appliance ASA.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'autorità di certificazione sull'appliance ASA fornisce le seguenti funzionalità:

- Integra le operazioni di base dell'autorità di certificazione sull'appliance ASA.
- Distribuisce i certificati.
- Consente di verificare in modo sicuro le revoche dei certificati rilasciati.
- Fornisce un'autorità di certificazione sull'appliance ASA per l'utilizzo con connessioni VPN SSL basate su browser (WebVPN) e client (AnyConnect).
- Fornisce agli utenti certificati digitali attendibili, senza la necessità di utilizzare l'autorizzazione di certificati esterni.
- Fornisce un'autorità interna sicura per l'autenticazione dei certificati e consente la semplice registrazione degli utenti tramite l'accesso a un sito Web.

Linee guida e limitazioni

- Supportato in modalità firewall instradato e trasparente.
- Su un'appliance ASA può essere residente un solo server CA locale alla volta.
- L'appliance ASA come funzionalità server CA locale non è supportata in una configurazione di failover.
- A partire da questo momento, l'appliance ASA funziona come server CA locale e supporta solo la generazione di certificati SHA1.
- Il server CA locale può essere utilizzato per connessioni VPN SSL basate su browser e client. Attualmente non supportato per IPSec.
- Il bilanciamento del carico VPN per la CA locale non è supportato.
- La CA locale non può essere subordinata a un'altra CA. Può fungere solo da CA radice.
- Al momento, l'appliance ASA non può registrare il certificato di identità sul server CA locale.

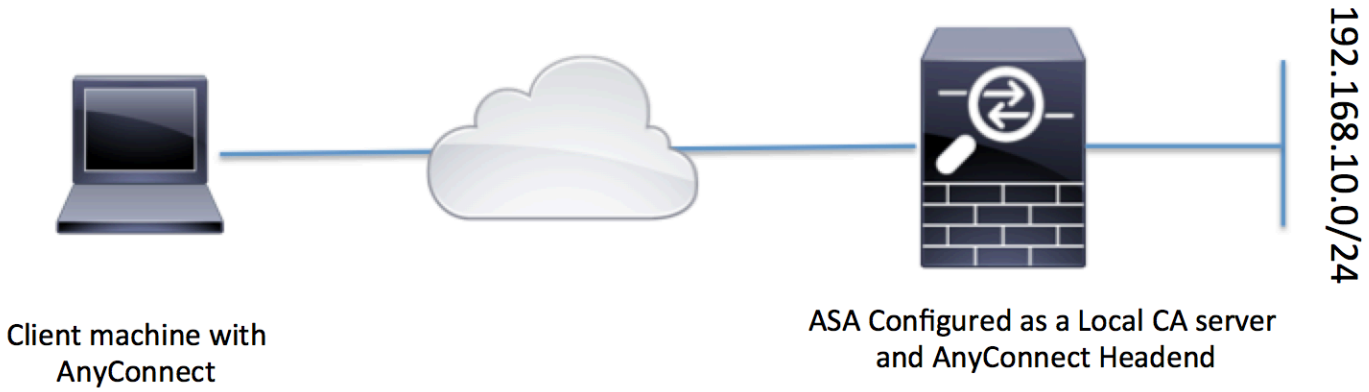
- Una volta completata la registrazione di un certificato, l'ASA memorizza un file PKCS12 contenente la coppia di chiavi e la catena di certificati dell'utente, che richiede circa 2 KB di memoria flash o di spazio su disco per registrazione. La quantità effettiva di spazio su disco dipende dalle dimensioni della chiave RSA e dai campi del certificato configurati. Tenere presente questa guida quando si aggiungono un numero elevato di registrazioni di certificati in sospeso su un'ASA con una quantità limitata di memoria flash disponibile, in quanto questi file PKCS12 vengono archiviati nella memoria flash per la durata del timeout di recupero della registrazione configurato.

Configurazione

In questa sezione viene descritto come configurare Cisco ASA come server CA locale.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

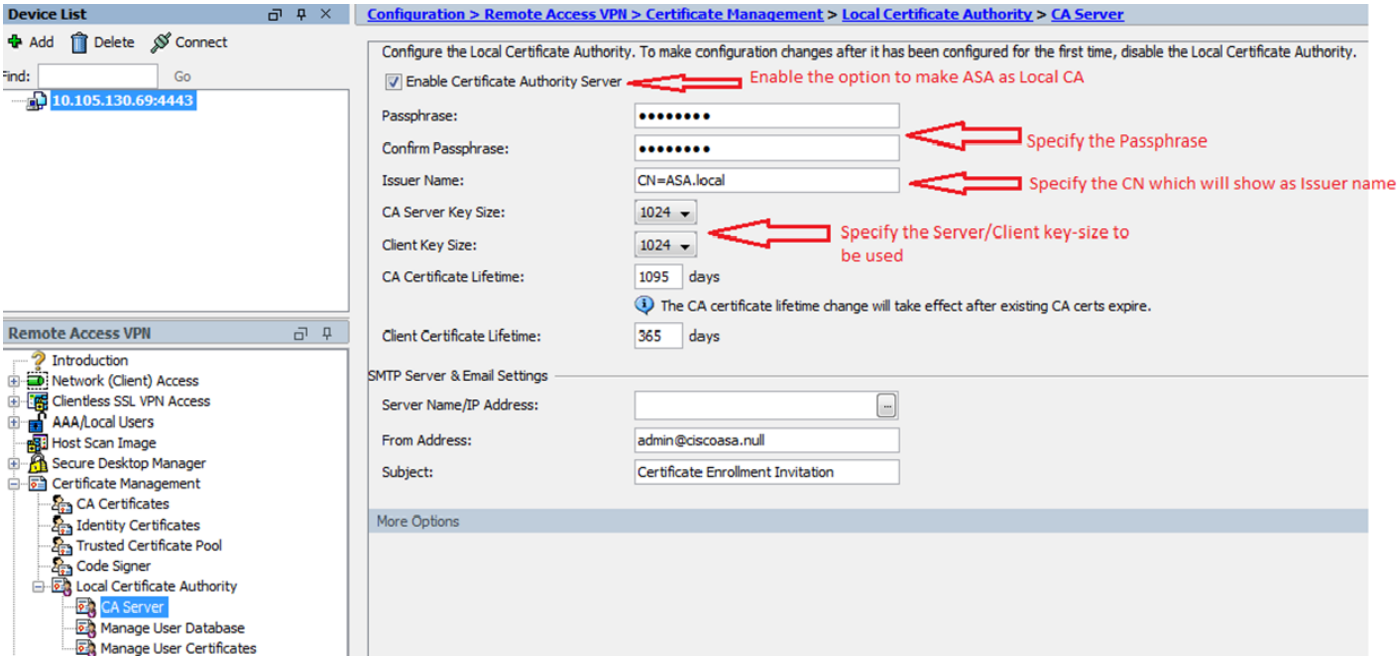


ASA come server CA locale

Passaggio 1. Configurare e abilitare il server CA locale su ASA

- Passare a Configurazione > VPN Accesso remoto > Gestione certificati > Autorità di certificazione locale > Server CA. Selezionare l'opzione Abilita server Autorità di certificazione.
- Configurare la passphrase. La passphrase deve essere composta da un minimo di 7 caratteri, utilizzati per codificare e salvare un file PKCS12 che include il certificato CA locale e la coppia di chiavi. La passphrase sblocca l'archivio PKCS12 in caso di perdita del certificato CA o della tastiera.

- Configurare il nome dell'autorità emittente. Questo campo viene visualizzato come CN certificato radice. Tale valore può essere specificato nel seguente formato: CN (Nome comune), OU (Unità organizzativa), O (Organizzazione), L (Località), S (Stato) e C (Paese).
- Configurazione facoltativa: configurare le impostazioni del server SMTP e del server di posta elettronica per garantire che OTP possa essere ricevuto dai client finali tramite posta elettronica per completare la registrazione. È possibile configurare il nome host o l'indirizzo IP del server di posta elettronica/SMTP locale. È inoltre possibile configurare i campi Indirizzo mittente e Oggetto dell'e-mail che i client riceveranno. Per impostazione predefinita, il campo Dall'indirizzo è admin@<nome host ASA>.null e il campo Oggetto è Invito a registrazione certificato.
- Configurazione facoltativa: è possibile configurare i parametri facoltativi quali dimensioni della chiave del client, dimensioni della chiave del server CA, durata del certificato CA e durata del certificato client.



Equivalente nella 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
```

Si tratta di campi aggiuntivi che è possibile configurare nella configurazione del server CA locale.

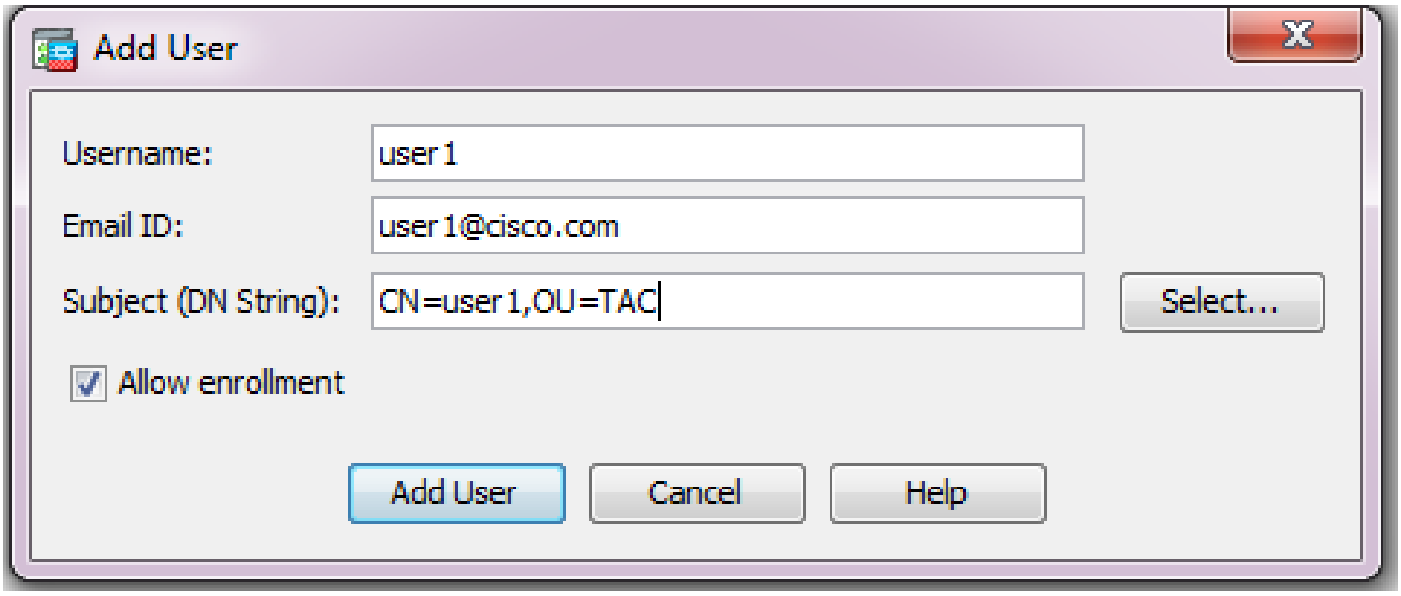
URL punto di distribuzione CRL	Questa è la posizione del CRL sull'appliance ASA. Il percorso predefinito è http://hostname.domain/+CSCOCA+/asa_ca.crl, ma è possibile modificare l'URL.
Interfaccia e porta Publish-CRL	Per rendere disponibile il CRL per il download HTTP su una determinata interfaccia e porta, scegliere un'interfaccia publish-CRL dall'elenco a discesa. Immettere quindi il numero di porta, che può essere qualsiasi numero di porta compreso tra 1 e 65535. Il numero di porta predefinito è la porta TCP 80.
Durata CRL	La CA locale aggiorna e riemette il CRL ogni volta che un certificato utente viene revocato o annullato, ma se non vi sono modifiche di revoca, il CRL viene emesso di nuovo automaticamente una volta ogni durata del CRL, il periodo di tempo specificato con il comando crl lifetime durante la configurazione della CA locale. Se non si specifica una durata per la CRL, il periodo di tempo predefinito è sei ore.
Percorso di archiviazione del database	L'appliance ASA accede a informazioni sugli utenti, certificati emessi ed elenchi di revoche e li implementa utilizzando un database CA locale. Per impostazione predefinita, il database risiede nella memoria flash locale o può essere configurato per risiedere in un file system esterno montato e accessibile per l'appliance ASA.
Nome soggetto predefinito	Immettere un oggetto predefinito (stringa DN) da aggiungere a un nome utente nei certificati rilasciati. Gli attributi DN consentiti sono indicati nell'elenco seguente: ·CN (Nome comune)SN (Cognome) ·O (Nome organizzazione) ·L (Località) ·C (Paese) ·Unitàorganizzativa ·EA (indirizzo e-mail) ·ST (Stato/Provincia) ·T (Titolo)
Periodo di iscrizione	Imposta il limite di tempo di registrazione in ore entro il quale l'utente può

	recuperare il file PKCS12 da ASA. Il valore predefinito è 24 ore. **Nota:** se il periodo di registrazione scade prima che l'utente recuperi il file PKCS12 che include il certificato utente, l'iscrizione non è consentita.
Scadenza password monouso	Definisce il periodo di tempo in ore durante il quale la registrazione OTP è valida per l'utente. Questo periodo di tempo inizia quando all'utente è consentita la registrazione. Il valore predefinito è 72 ore.
Promemoria scadenza certificato	Specifica il numero di giorni prima della scadenza del certificato durante i quali viene inviato un promemoria iniziale ai proprietari del certificato.

Passaggio 2. Creazione e aggiunta di utenti al database ASA

- Passare a Configurazione > VPN Accesso remoto > Gestione certificati > Autorità di certificazione locale > Gestisci database utenti.Fare clic su Aggiungi.

- Specificare i dettagli dell'utente, ovvero il nome utente, l'ID e-mail e il nome dell'oggetto, come illustrato in questa immagine.



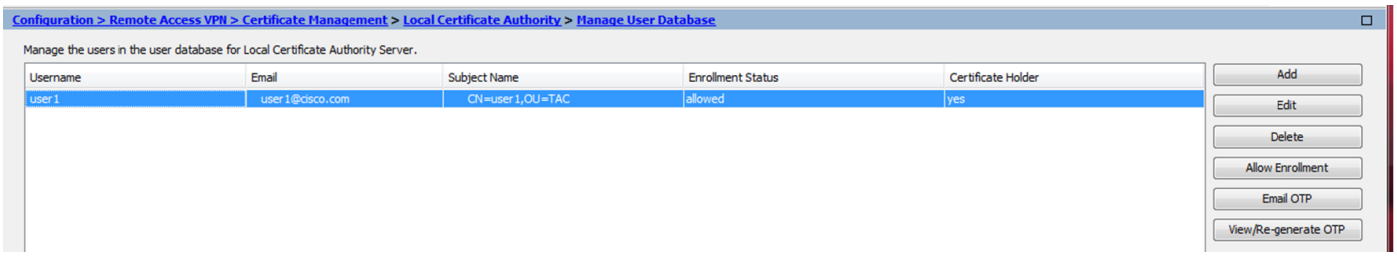
- Verificare che l'opzione Consenti registrazione sia selezionata per consentire la registrazione del certificato.
- Fare clic su Aggiungi utente per completare la configurazione utente.

Equivalente nella CLI:

<#root>

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

- Dopo l'aggiunta dell'utente al database utenti, lo stato di registrazione viene visualizzato come Consentito alla registrazione.



CLI per verificare lo stato utente:

<#root>

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:
```

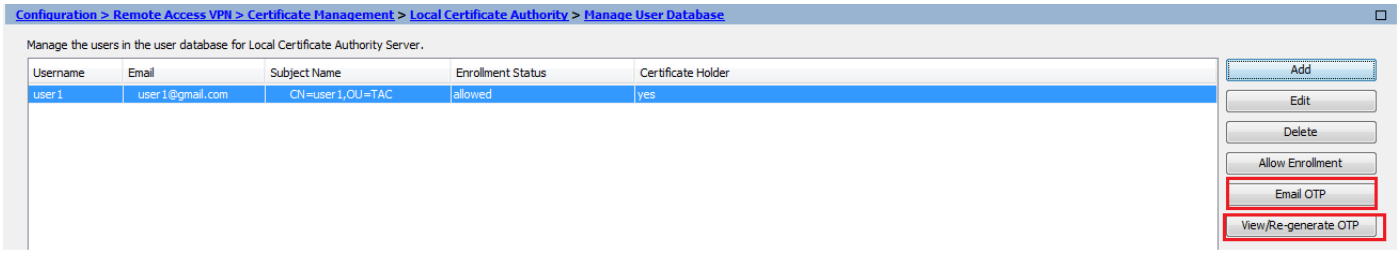
Allowed to Enroll

- Dopo aver aggiunto l'utente al database utenti, è possibile fornire la password per una sola volta (OTP), necessaria per completare la registrazione, utilizzando uno dei metodi seguenti:

Invia messaggio di posta elettronica all'OTP (è necessario che il server SMTP e le impostazioni di posta elettronica siano configurati nella configurazione del server CA).

O

Visualizzare direttamente OTP e condividere con l'utente facendo clic su Visualizza/rigenera OTP. Questa opzione può essere utilizzata anche per rigenerare l'OTP.



Equivalente nella CLI:

```
!! Email the OTP to the user
ASA# crypto ca server user-db allow user1 email-otp

!! Display the OTP on terminal
ASA# crypto ca server user-db allow user1 display-otp
Username: user1
OTP: 18D14F39C8F3DD84
Enrollment Allowed Until: 14:18:34 UTC Tue Jan 12 2016
```

Passaggio 3. Abilitare webvpn sull'interfaccia WAN

- Abilitare l'accesso Web sull'appliance ASA per permettere ai client di richiedere la registrazione.

```
!! Enable web-access on the "Internet" interface of the ASA
ASA(config)# webvpn
ASA(config-webvpn)#enable Internet
```

Passaggio 4. Importa il certificato nel computer client

- Nella workstation client aprire un browser e passare al collegamento per completare l'iscrizione.
- L'IP/FQDN utilizzato in questo collegamento deve essere l'IP dell'interfaccia su cui è abilitato

webvpn in questo passaggio, ossia l'interfaccia Internet.

<#root>

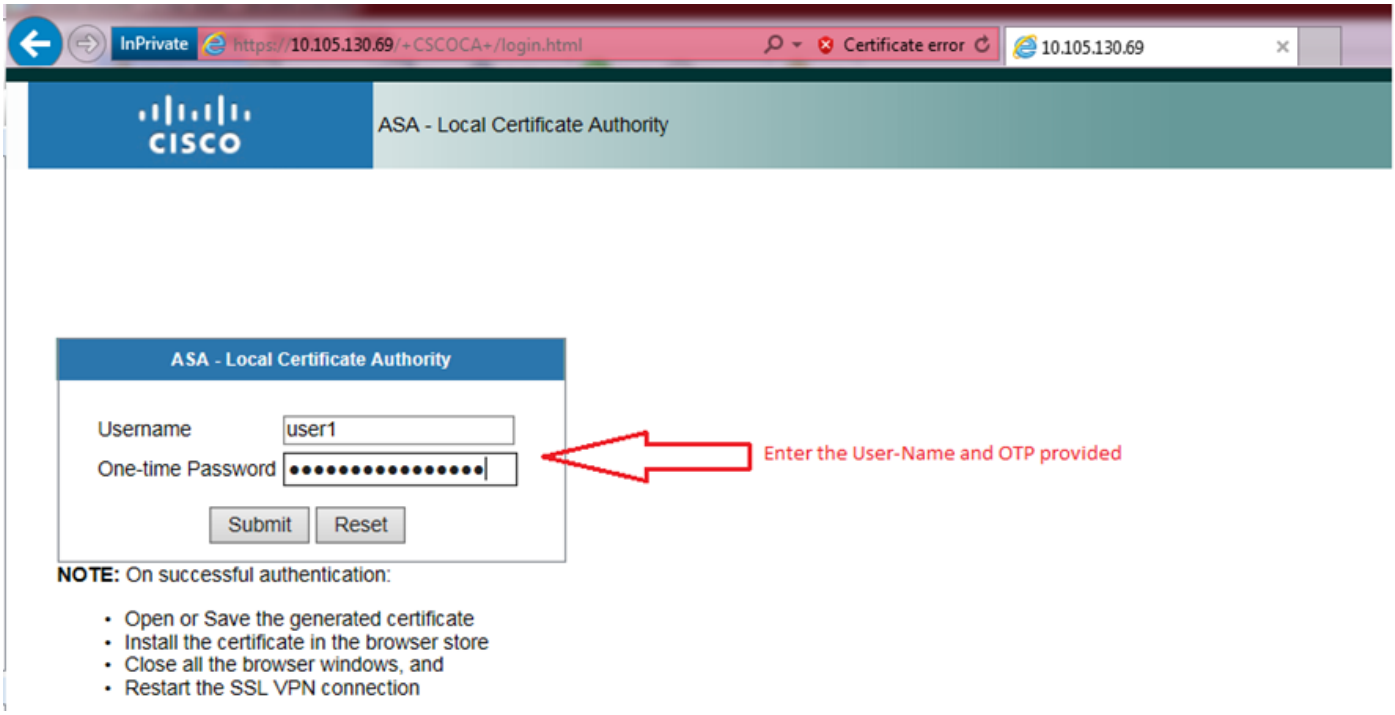
https://

<>

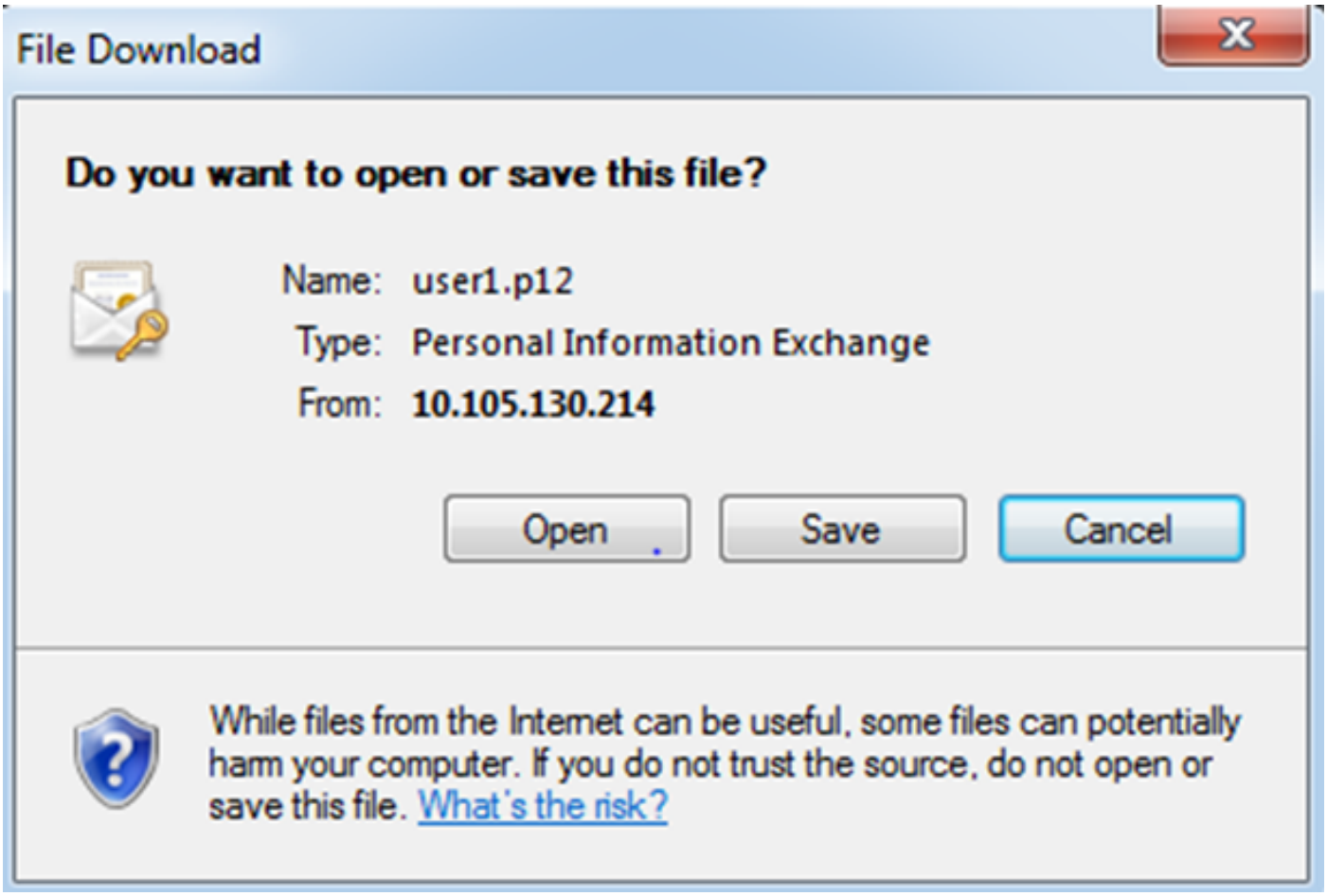
IP/FQDN>/+CSCOCA+/enroll.html

<>

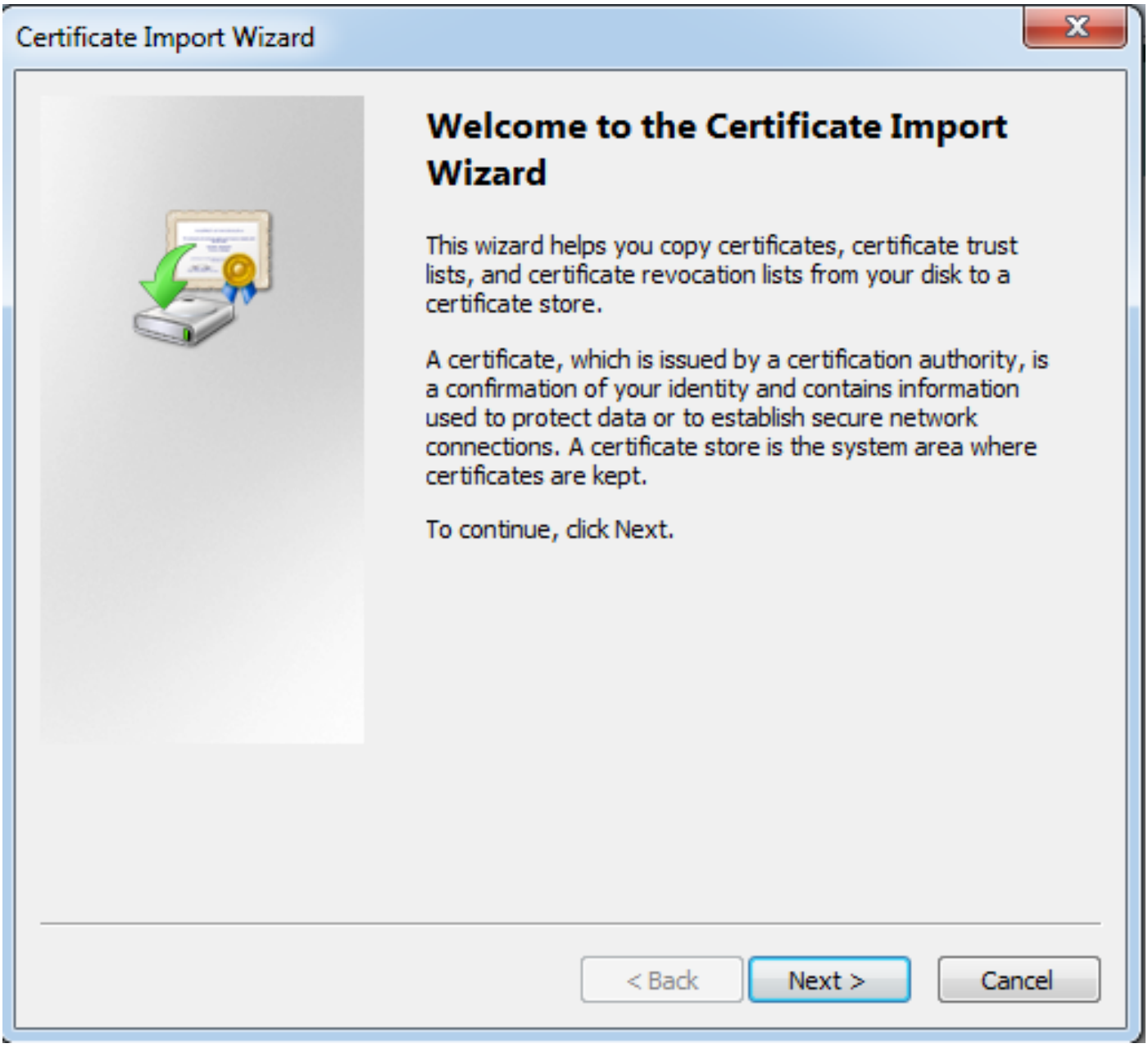
- Immettere il nome utente (configurato sull'appliance ASA nel passaggio 2, opzione A) e l'indirizzo OTP, fornito tramite e-mail o manualmente.



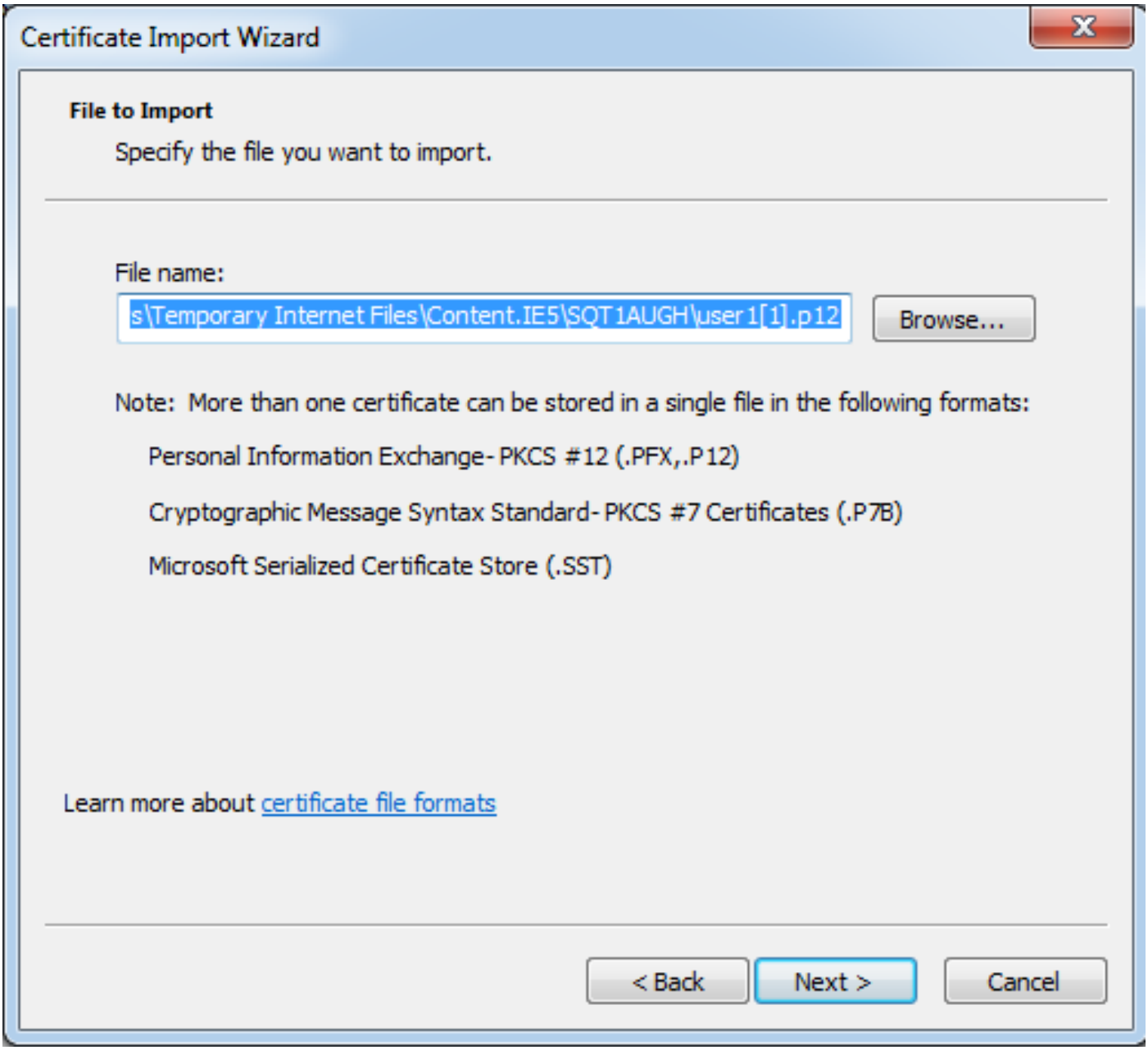
- Fare clic su Open per installare direttamente il certificato client ricevuto dall'appliance ASA.
- La passphrase per installare il certificato client è uguale a quella ricevuta in precedenza da OTP.



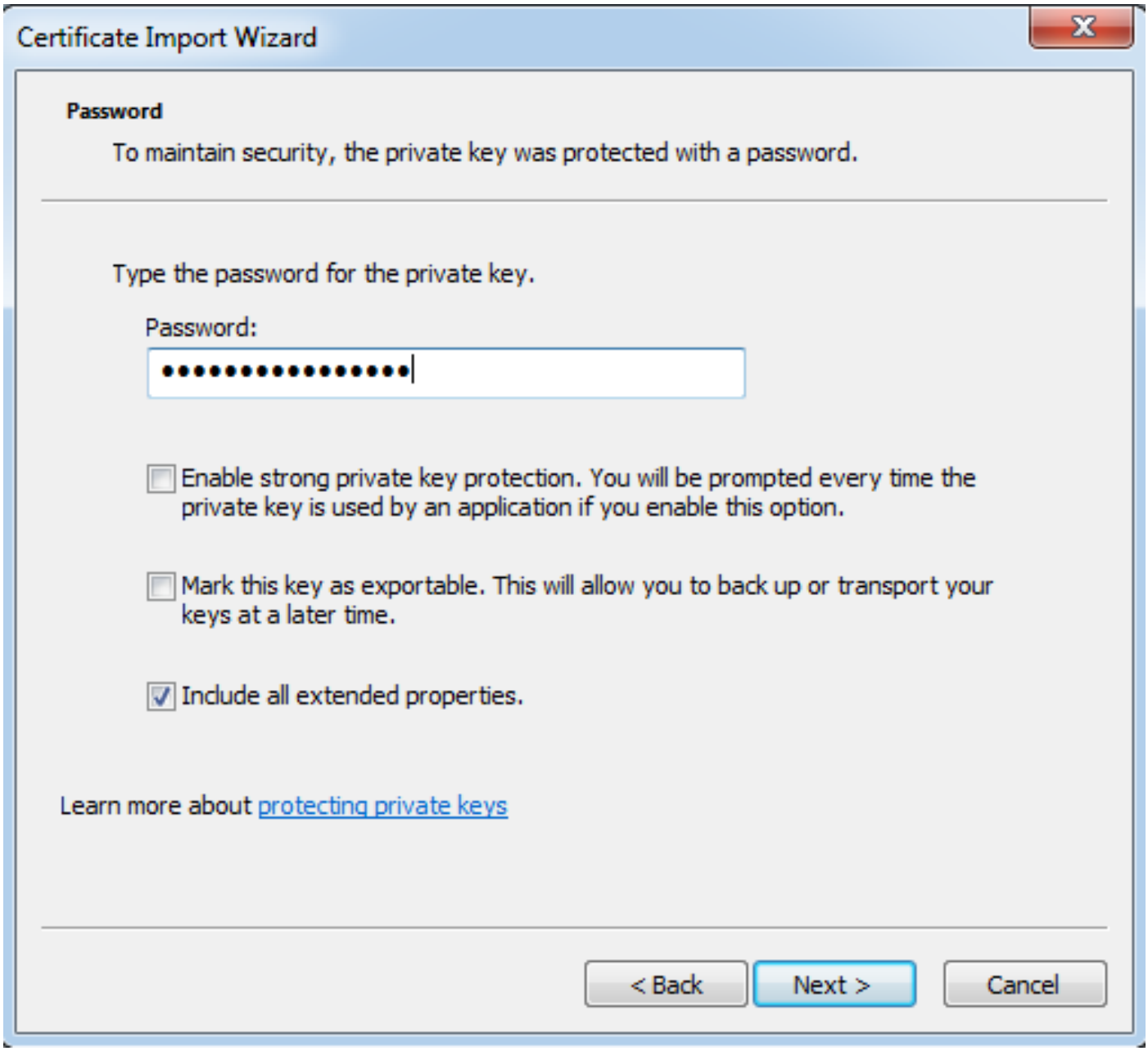
- Fare clic su Next (Avanti).



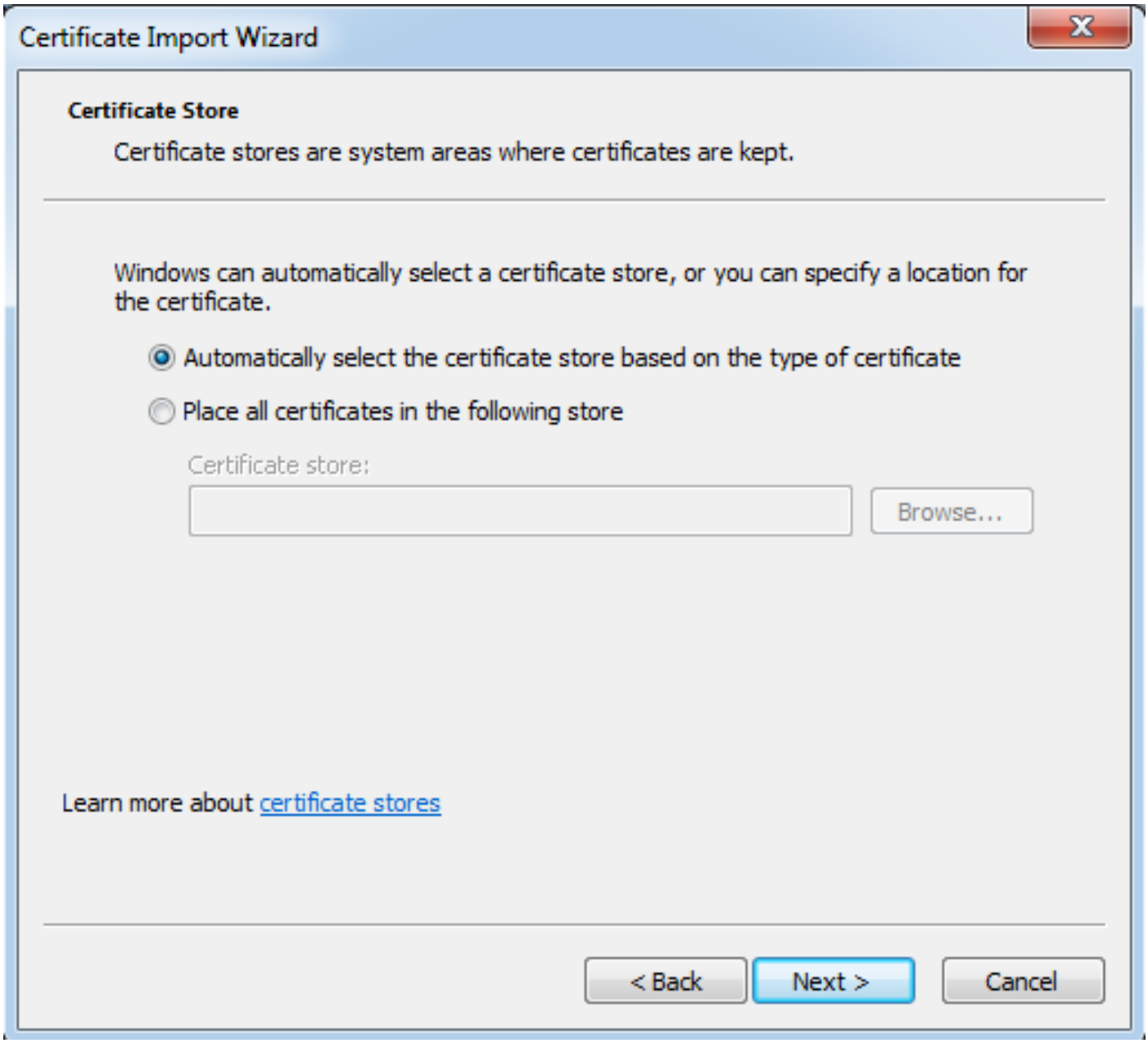
- Accettate il percorso di default e fate clic su Succ (Next).



- Immettere OTP nel campo Password.
- È possibile selezionare l'opzione Contrassegna questa chiave come esportabile in modo che la chiave possa essere esportata dalla workstation in futuro, se necessario.
- Fare clic su Avanti.



- È possibile installare manualmente il certificato in un determinato archivio certificati oppure lasciare che scelga automaticamente l'archivio.
- Fare clic su Next (Avanti).



- Per completare l'installazione, fare clic su Finish (Fine).

Certificate Import Wizard

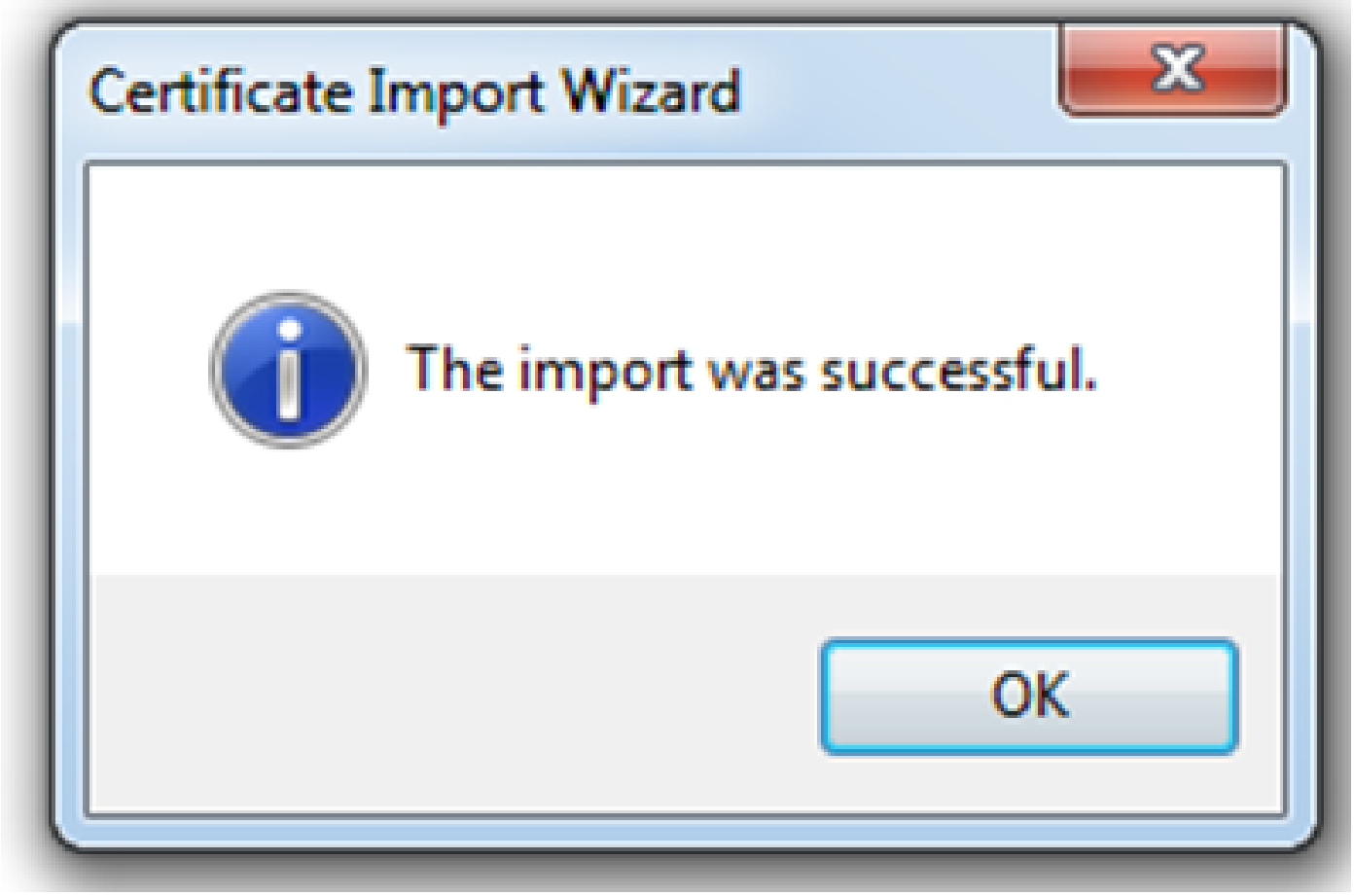
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

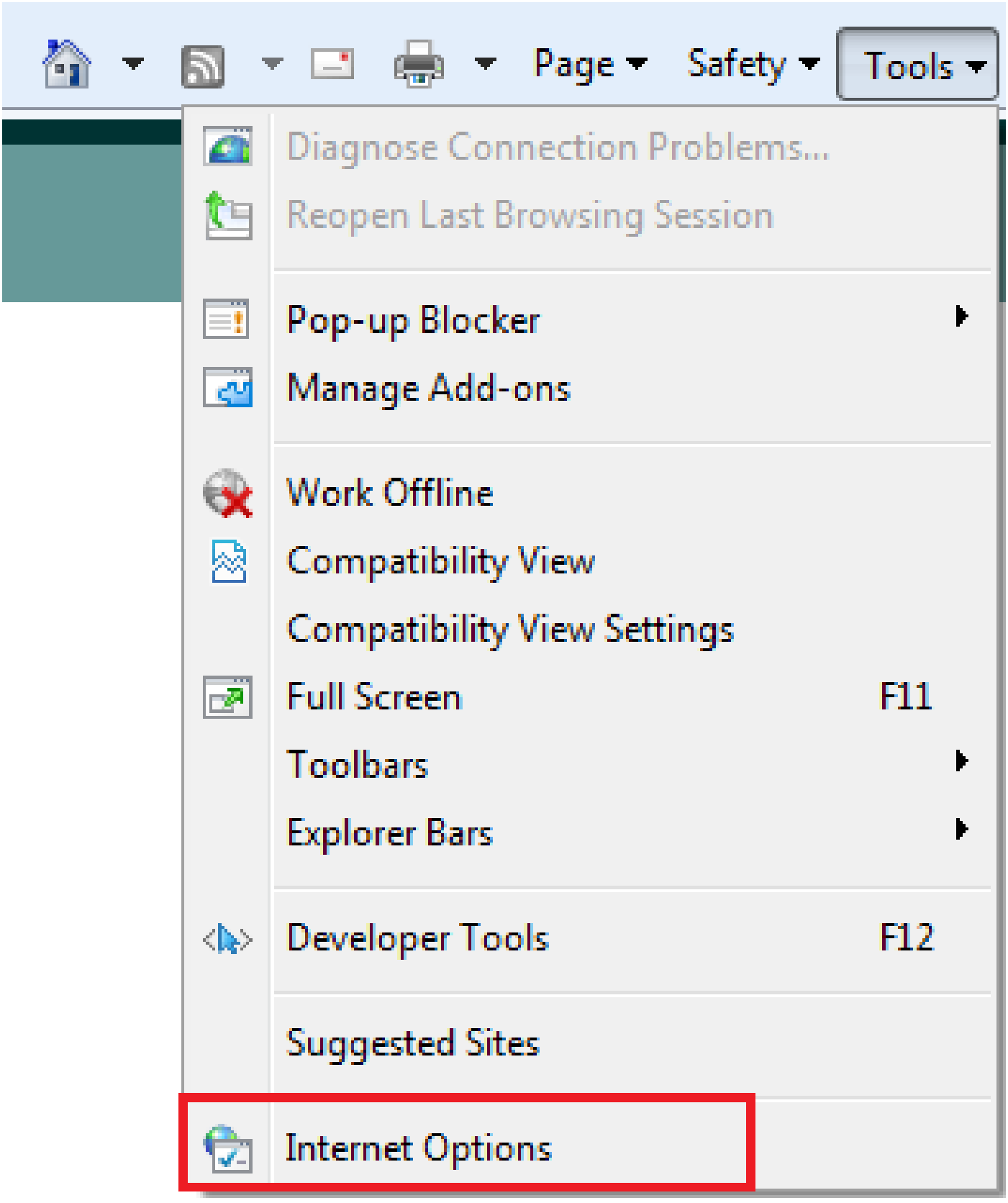
You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	PFX
File Name	C:\Users\mrsethi\AppData\Lo

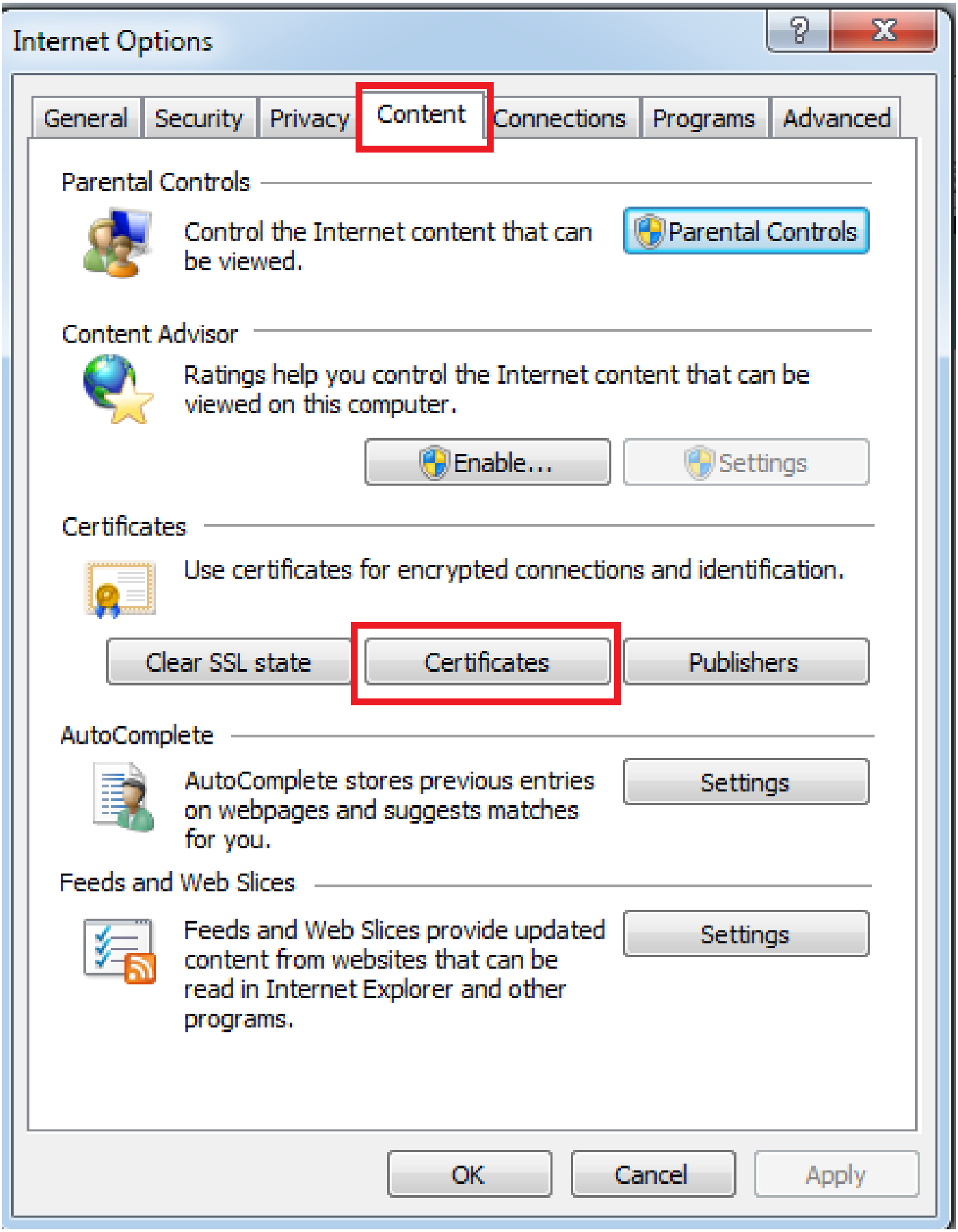
< Back | Finish | Cancel



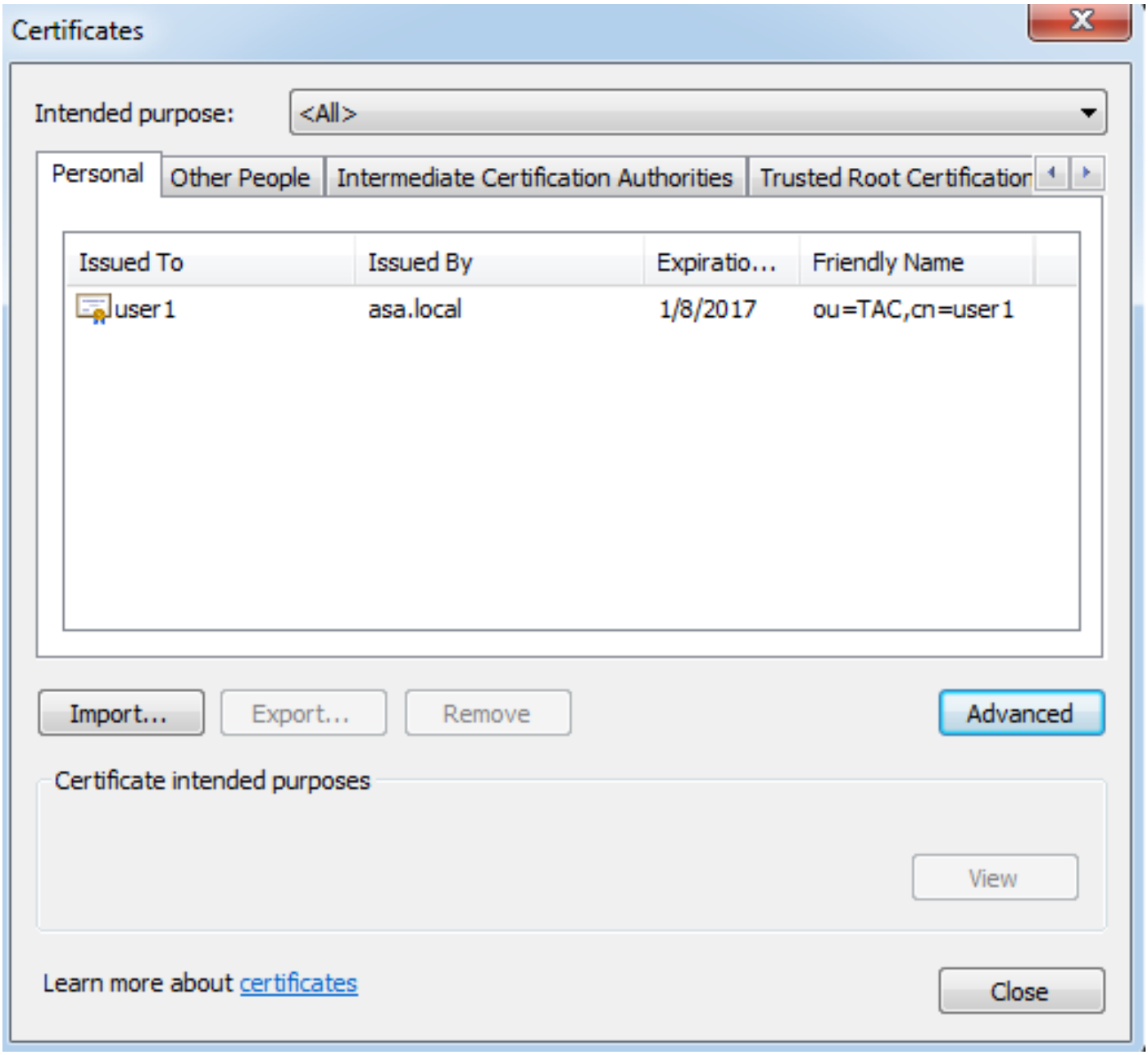
- Una volta installato correttamente il certificato, è possibile verificarlo.
- Aprire Internet Explorer e selezionare Strumenti > Opzioni Internet.



- Passare alla scheda Contenuto e fare clic su Certificati, come mostrato nell'immagine.



- Nell'archivio personale, è possibile visualizzare il certificato ricevuto dall'appliance ASA.



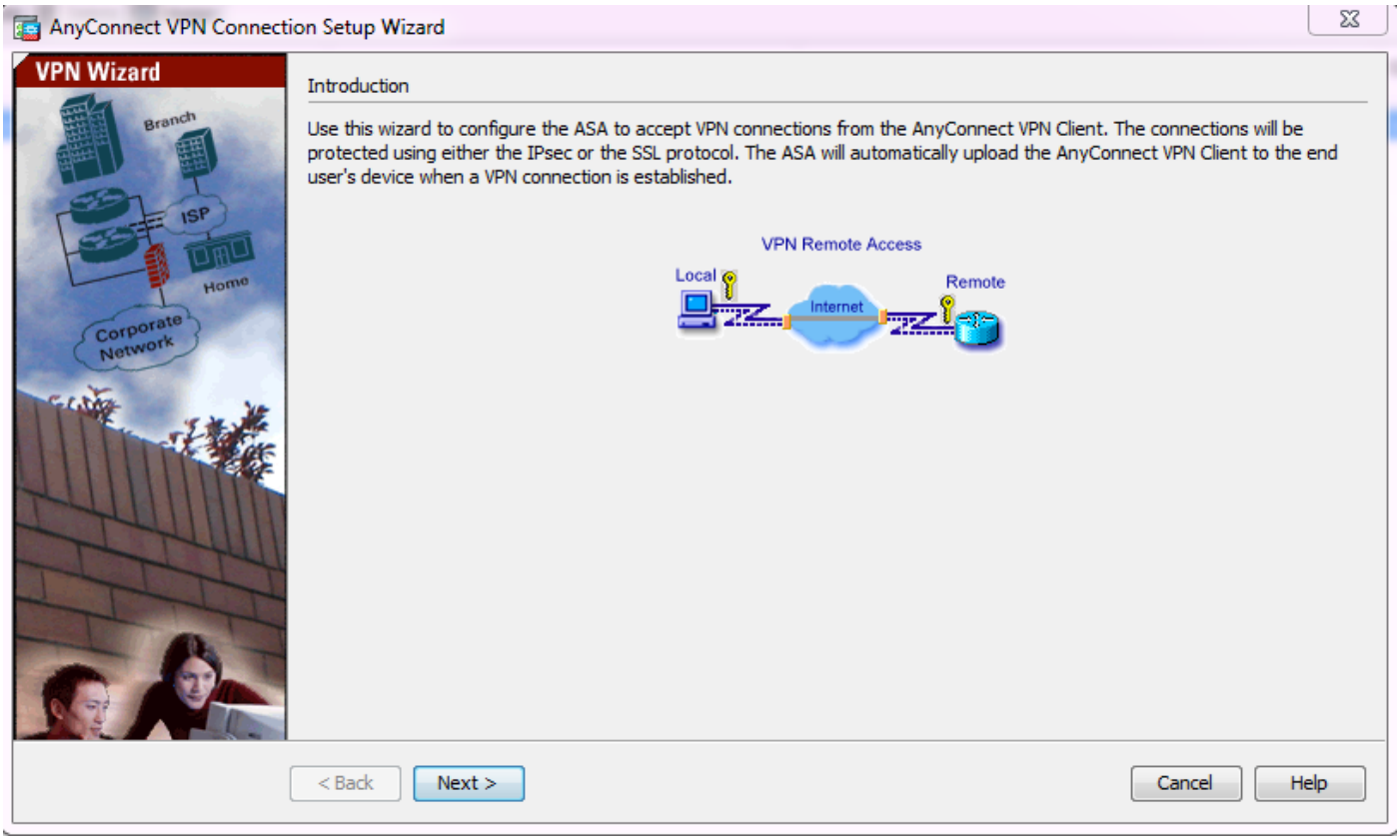
ASA come gateway SSL per i client AnyConnect

Configurazione guidata AnyConnect ASDM

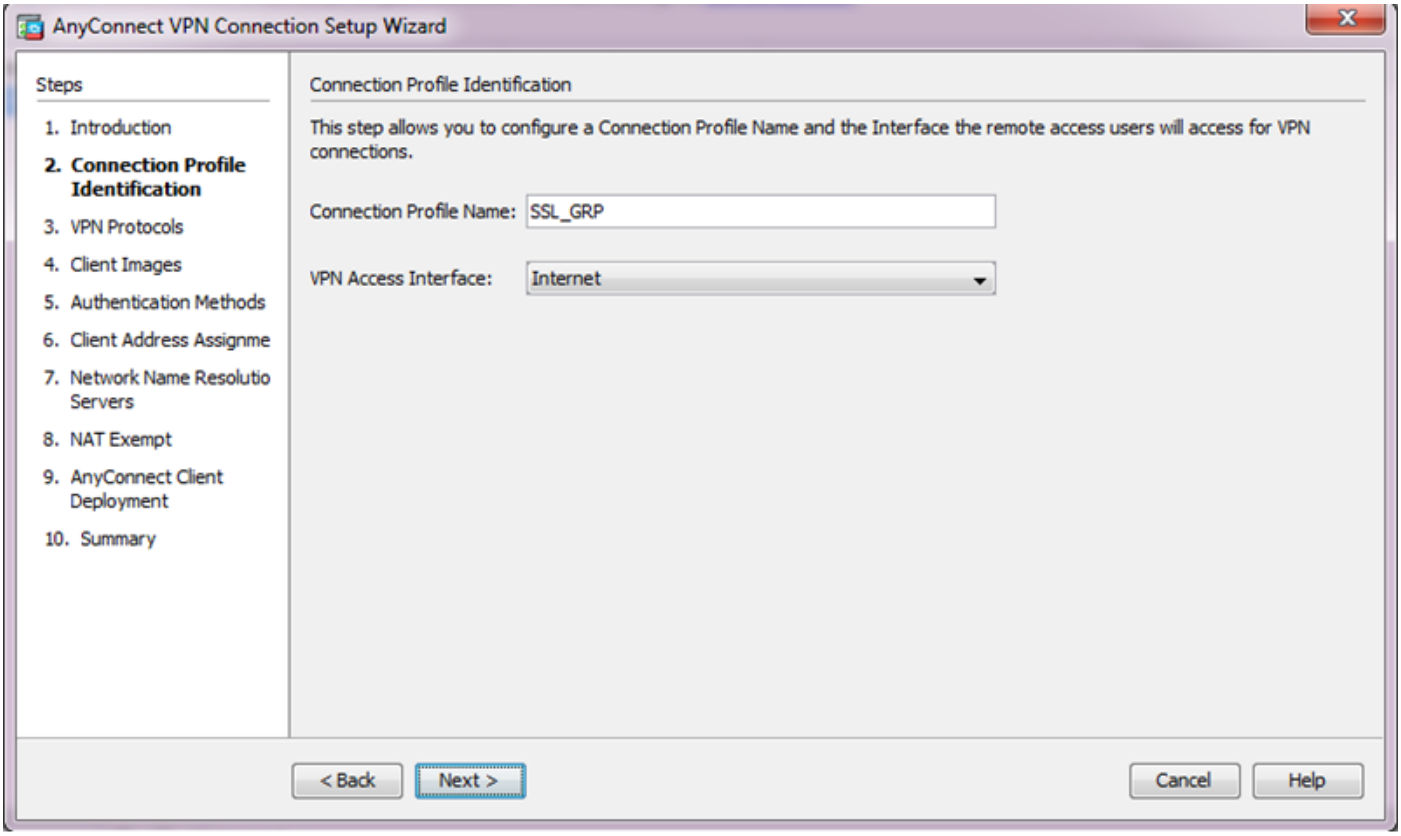
La configurazione guidata di AnyConnect/CLI può essere usata per configurare AnyConnect Secure Mobility Client. Prima di procedere, verificare che un pacchetto client AnyConnect sia stato caricato nella memoria flash/sul disco del firewall ASA.

Per configurare AnyConnect Secure Mobility Client tramite la Configurazione guidata, completare la procedura seguente:

1. Accedere ad ASDM e selezionare Wizards> VPN Wizards > AnyConnect VPN Wizard per avviare la Configurazione guidata e fare clic su Next (Avanti).



2. Immettere il nome del profilo di connessione, scegliere l'interfaccia su cui terminare la VPN dal menu a discesa Interfaccia di accesso VPN e fare clic su Avanti.



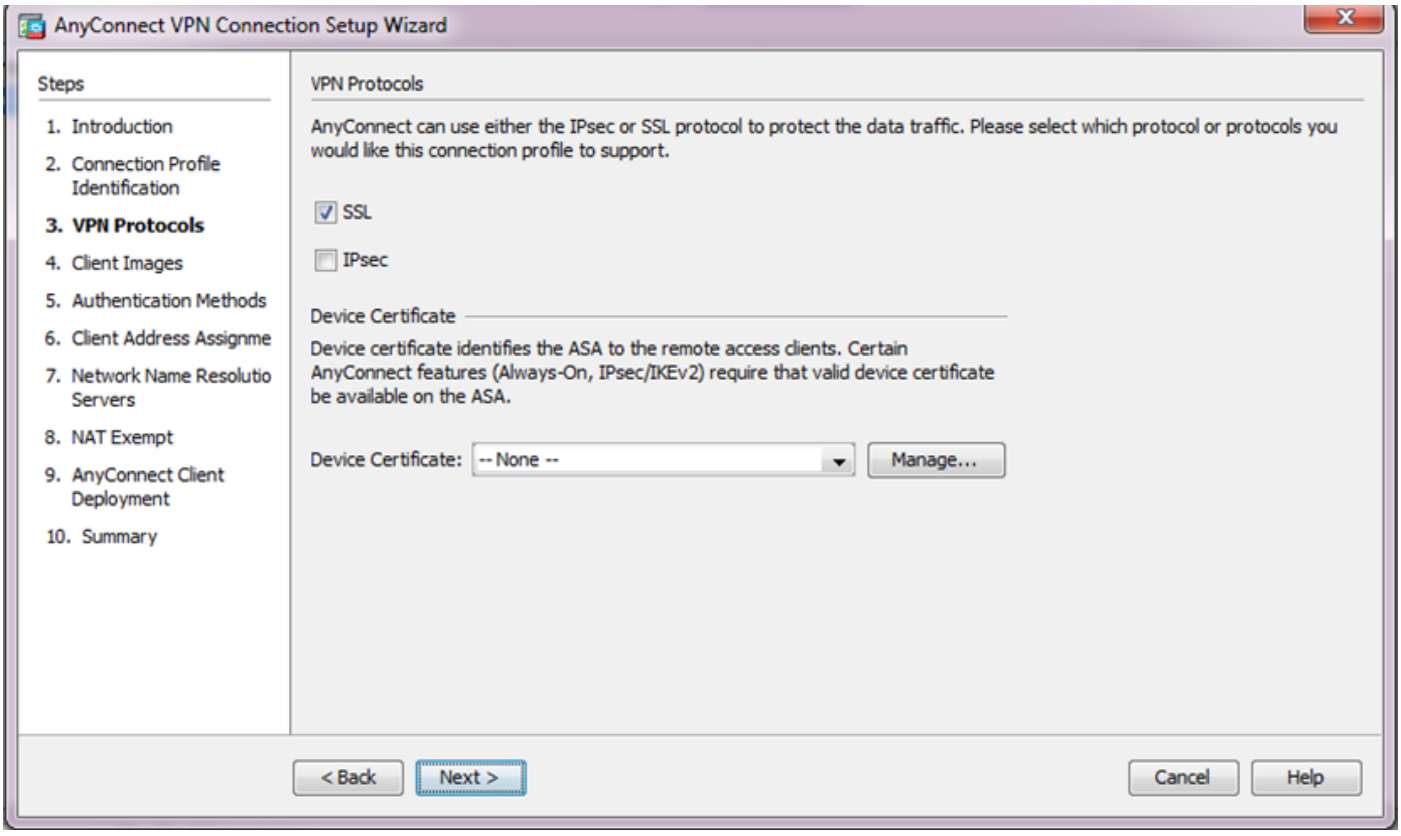
3. Selezionare la casella di controllo SSL per abilitare Secure Sockets Layer (SSL). Il certificato del dispositivo può essere un certificato rilasciato da un'Autorità di certificazione (CA) di terze parti attendibile, ad esempio Verisign o Entrust, oppure un certificato autofirmato. Se il certificato è già

installato sull'appliance ASA, può essere scelto tramite il menu a discesa.

1. Nota: questo certificato è il certificato sul lato server che verrà presentato dall'ASA ai client SSL. Se sull'appliance ASA non è installato alcun certificato server superiore alla generazione di un certificato autofirmato, fare clic su Gestisci.

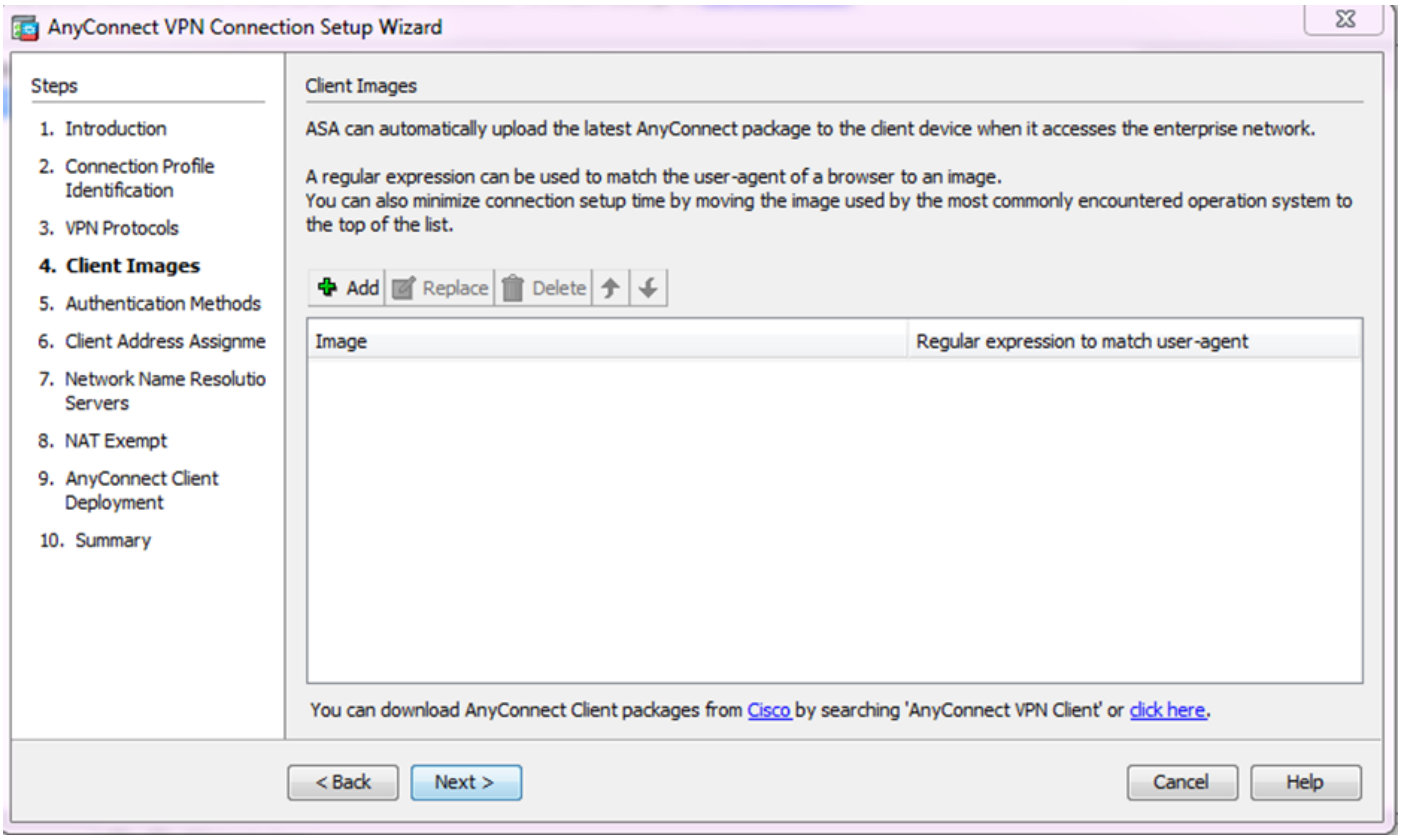
Per installare un certificato di terze parti, completare la procedura descritta nell'ASA 8.x Installazione manuale dei certificati dei fornitori di terze parti da utilizzare con la configurazione di WebVPN nel documento Cisco.

- Abilitare i protocolli VPN e il certificato dispositivo.
- Fare clic su Next (Avanti).

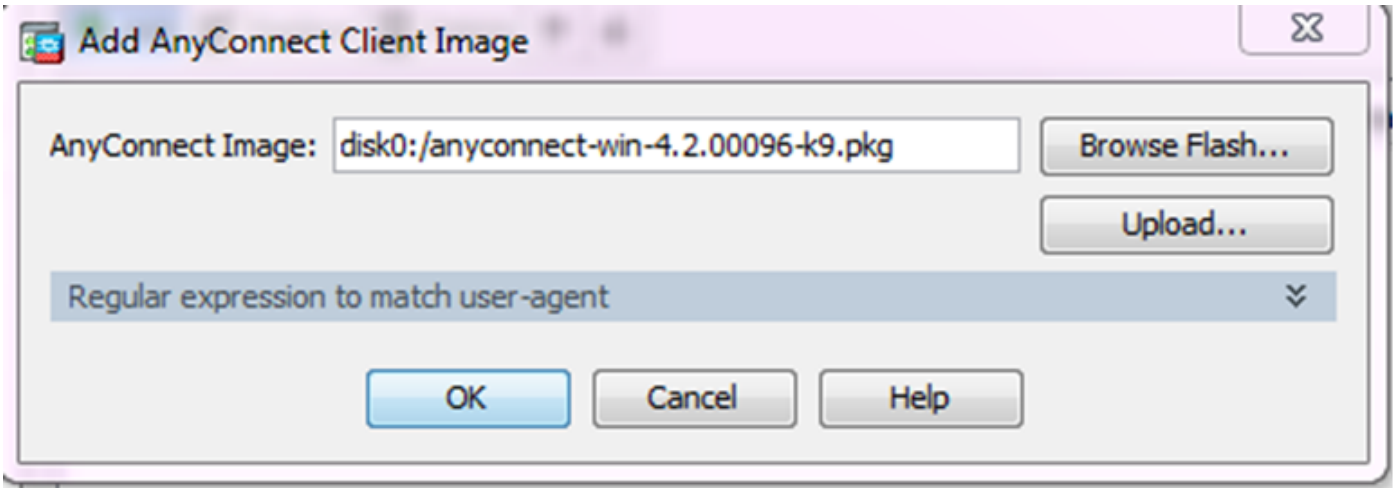


4. Fare clic su Add per aggiungere il pacchetto del client AnyConnect (file con estensione pkg) dall'unità locale o dal disco flash/disk dell'appliance ASA.

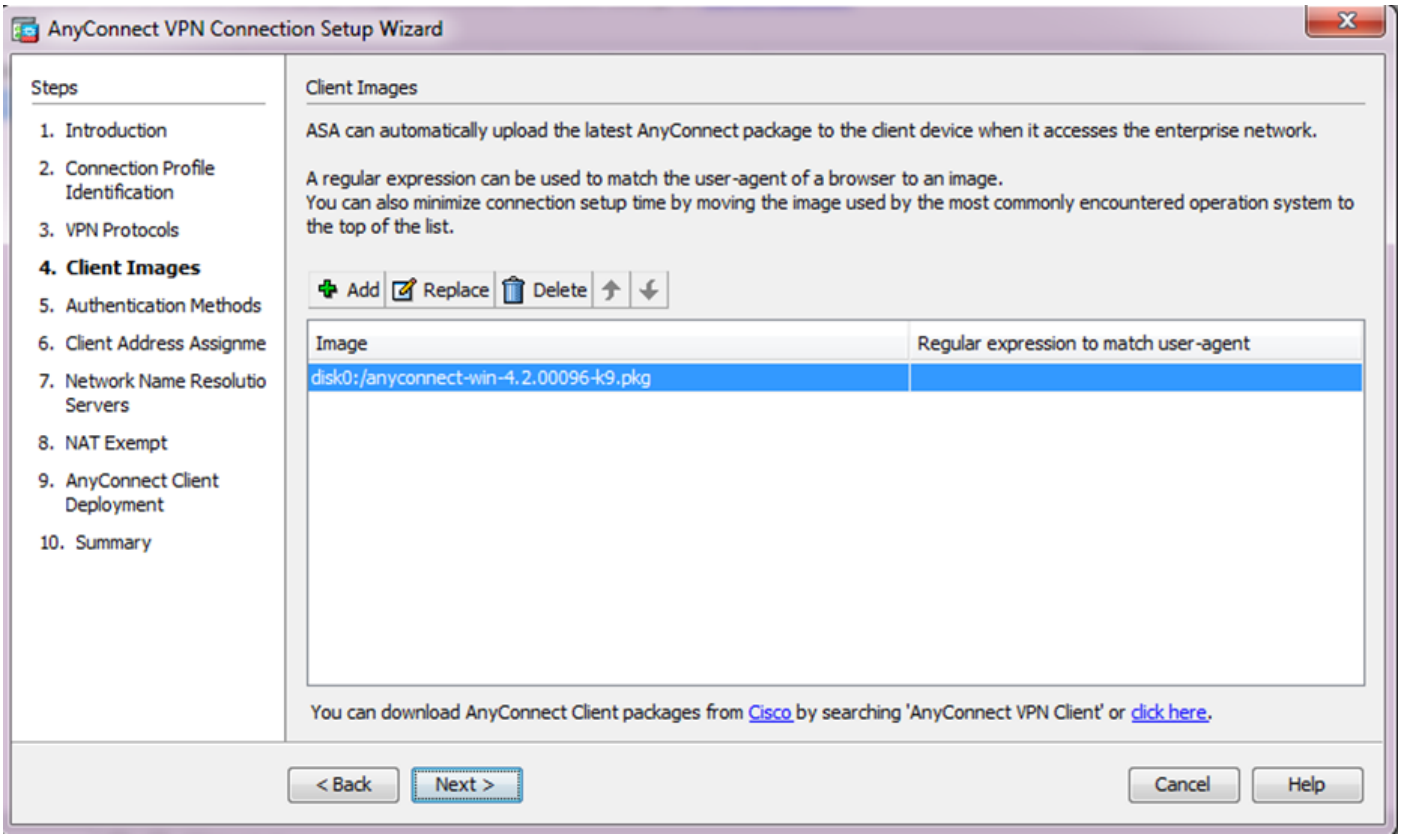
Fare clic su Browse Flash per aggiungere l'immagine dall'unità flash, oppure fare clic su Upload per aggiungere l'immagine dall'unità locale del computer host.



- È possibile caricare il file AnyConnect.pkg da ASA Flash/Disk (se il pacchetto è già presente) o dall'unità locale.
- Sfogliare flash - per selezionare il pacchetto AnyConnect da ASA Flash/Disk.
- Upload: per selezionare il pacchetto AnyConnect dall'unità locale del computer host.
- Fare clic su OK.

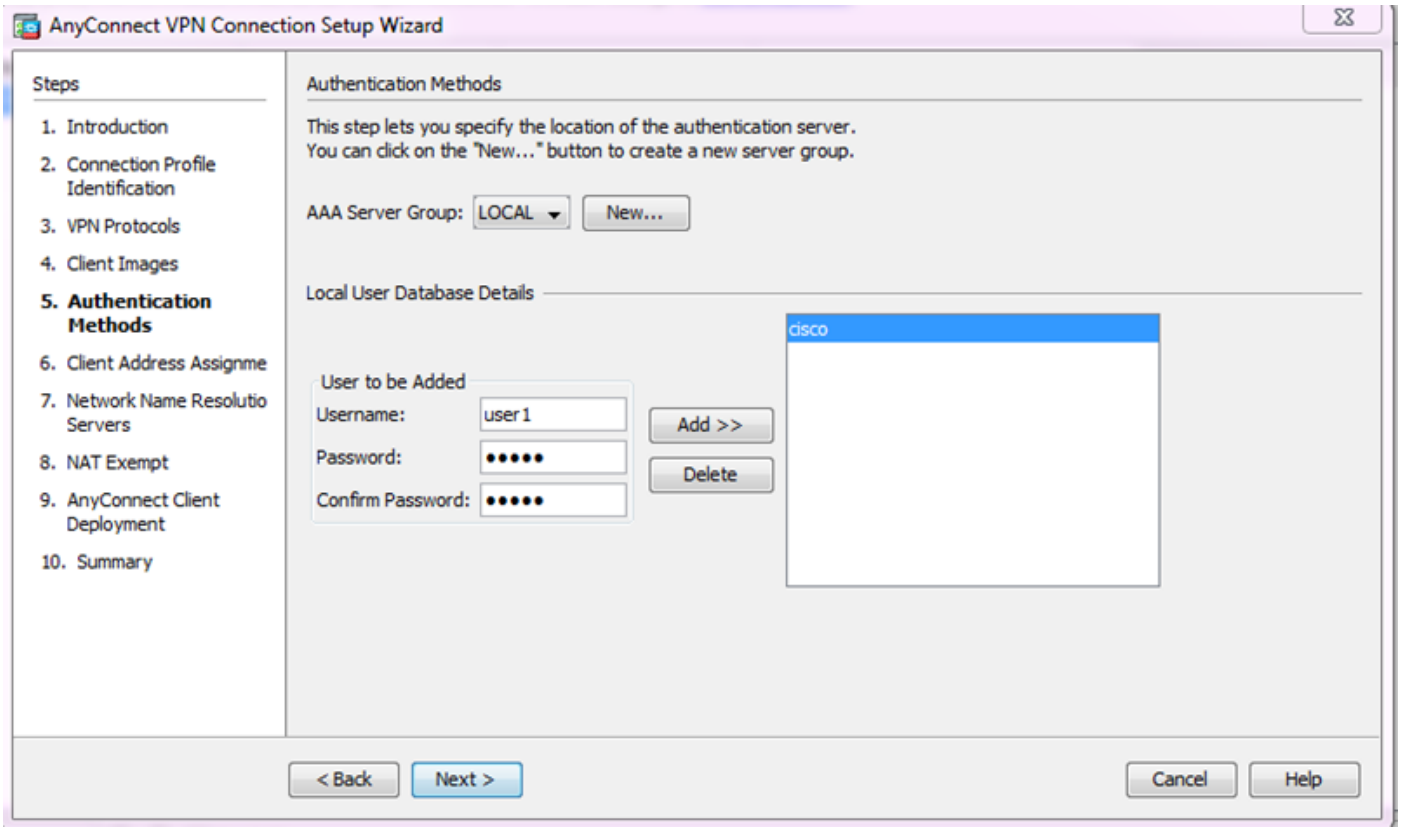


- Fare clic su Next (Avanti).

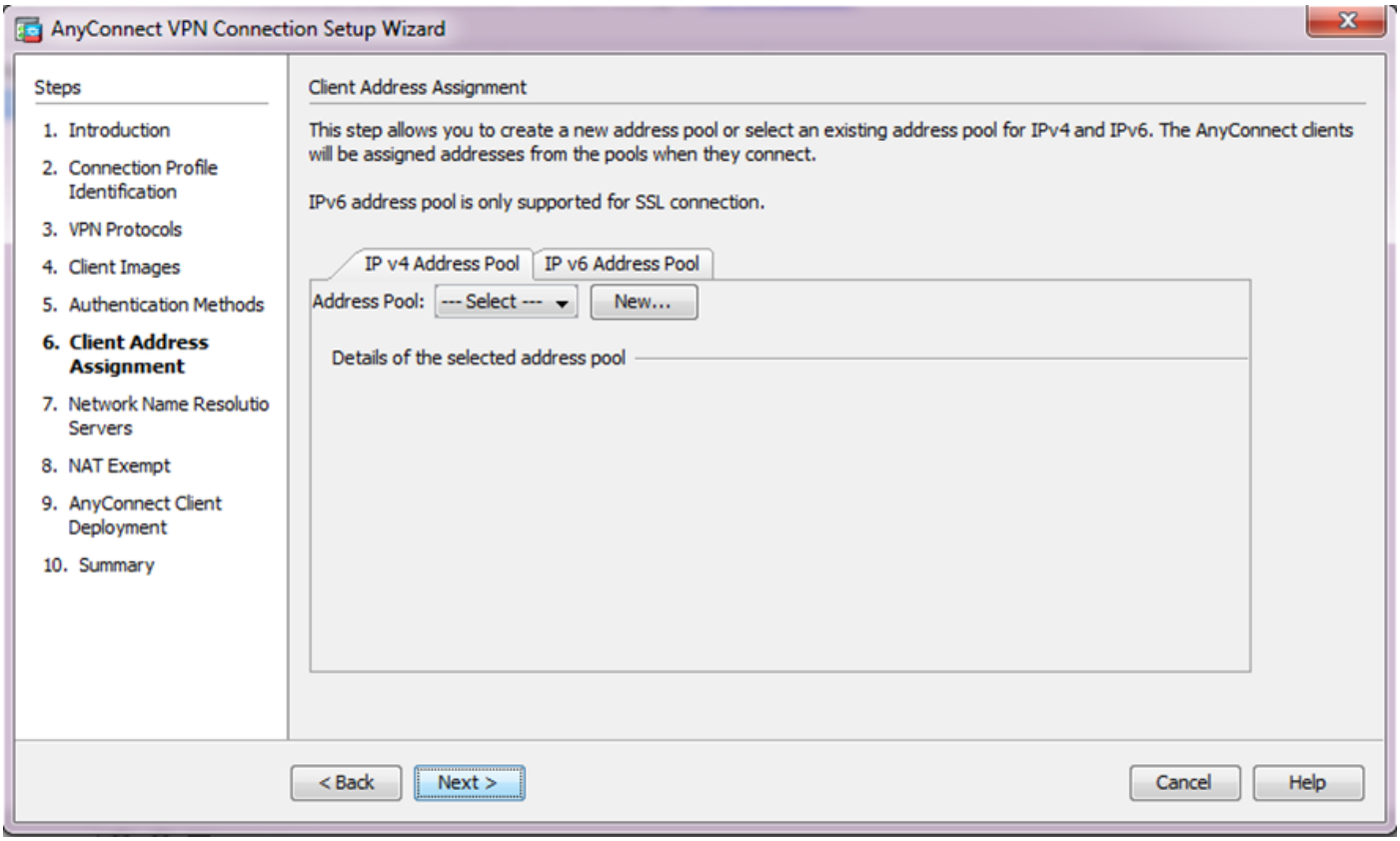


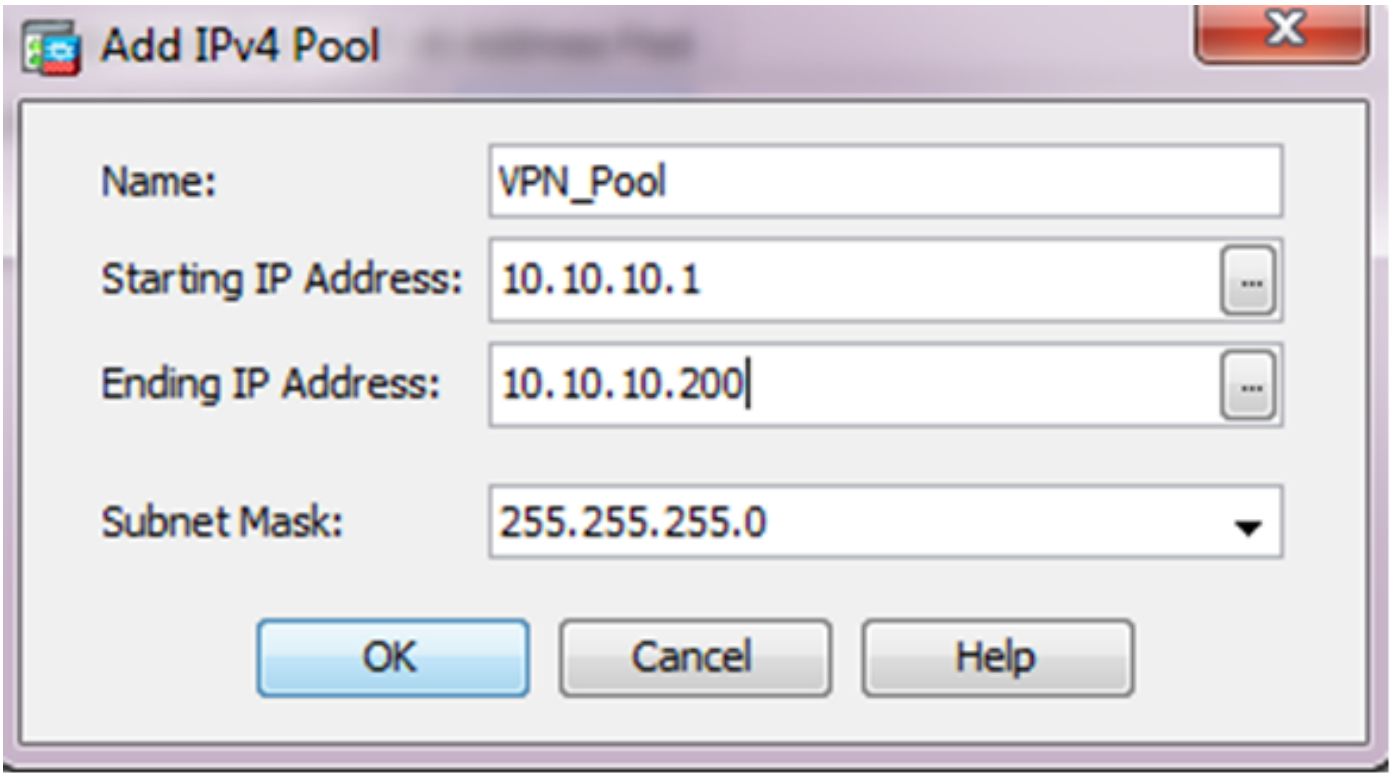
5. L'autenticazione dell'utente può essere completata tramite i gruppi di server Autenticazione, Autorizzazione e Contabilità (AAA). Se gli utenti sono già configurati, scegliere LOCAL, quindi fare clic su Next (Avanti). In caso contrario, aggiungere un utente al database degli utenti locali e fare clic su Avanti.

Nota: nell'esempio, è configurata l'autenticazione LOCAL, ossia per l'autenticazione verrà utilizzato il database utenti locale sull'appliance ASA.

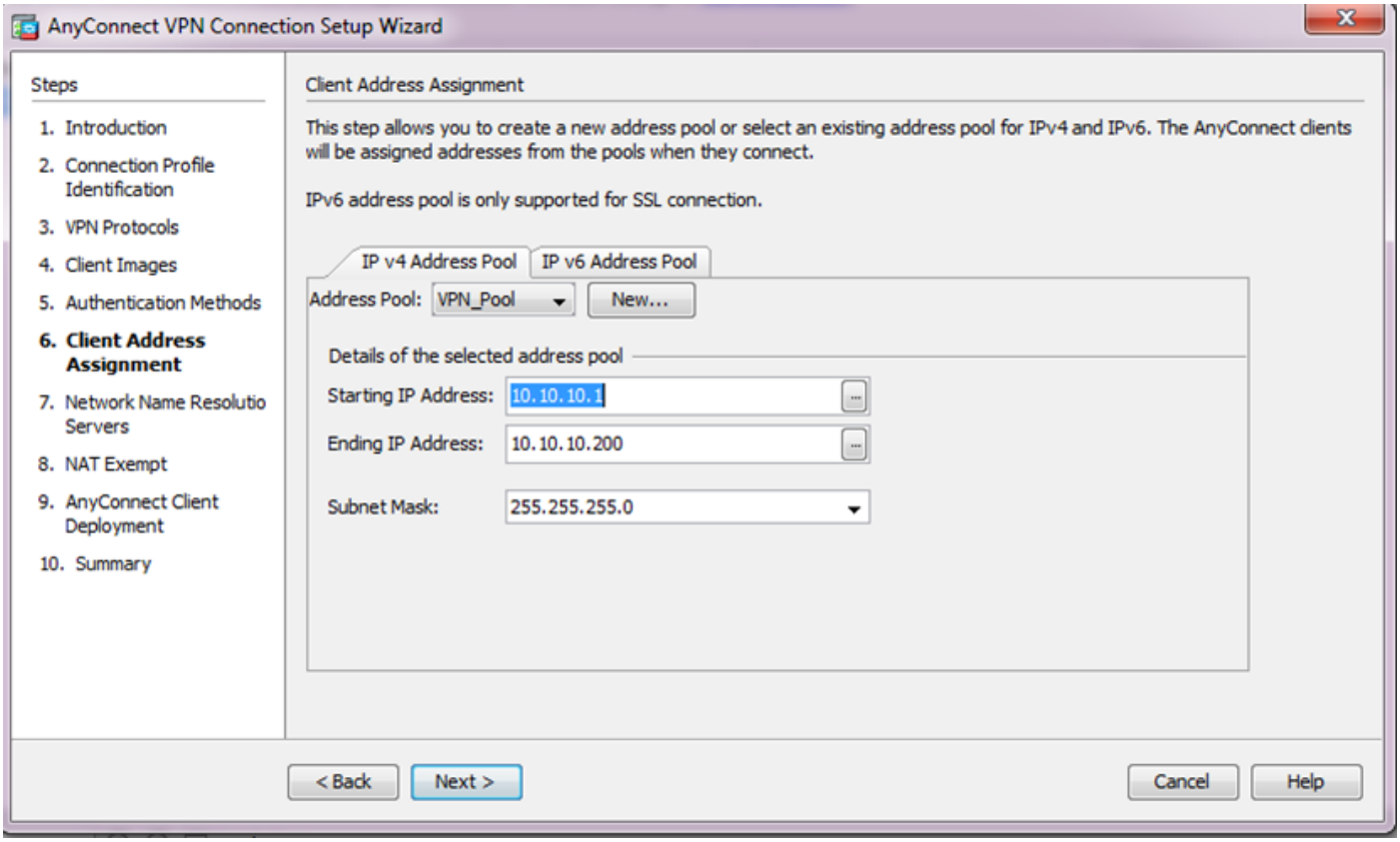


6. Verificare che il pool di indirizzi per i client VPN sia configurato. Se è già stato configurato un pool ip, selezionarlo dal menu a discesa. In caso contrario, fare clic su New (Nuovo) per eseguire la configurazione. Al termine, fare clic su Avanti.

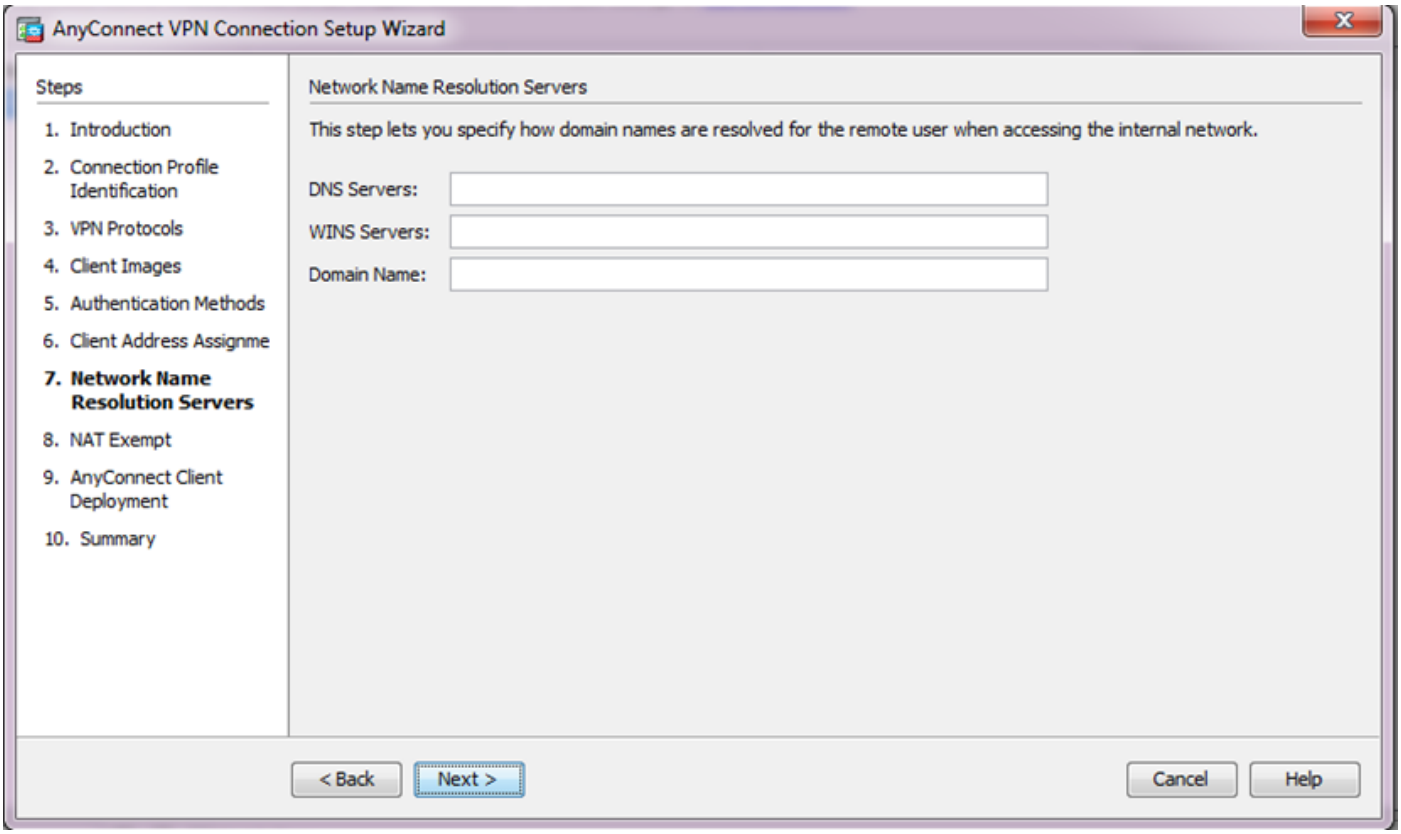




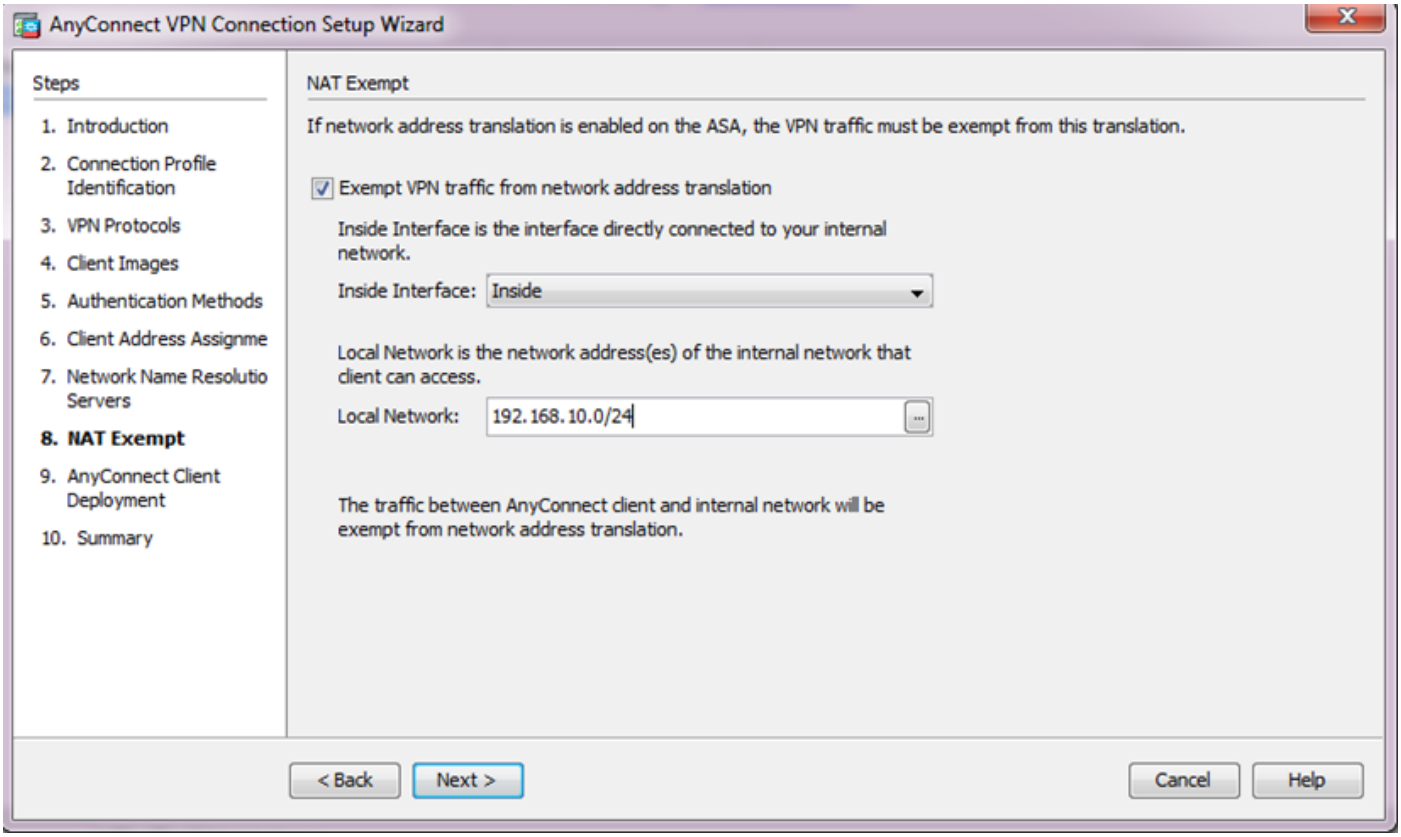
- Fare clic su Next (Avanti).



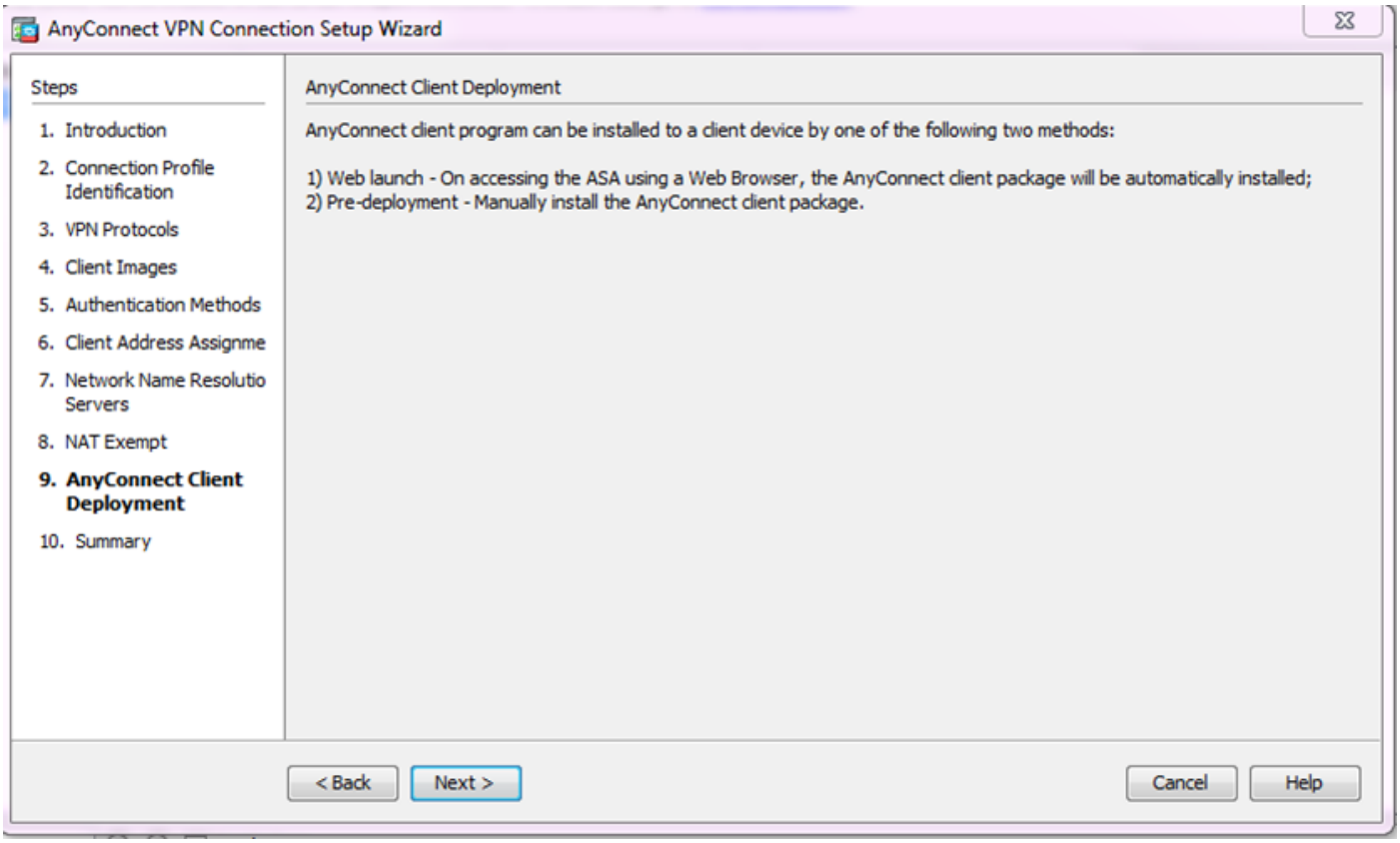
7. Facoltativamente, configurare i server DNS (Domain Name System) e i DN nei campi DNS e Nome dominio e quindi fare clic su Avanti.



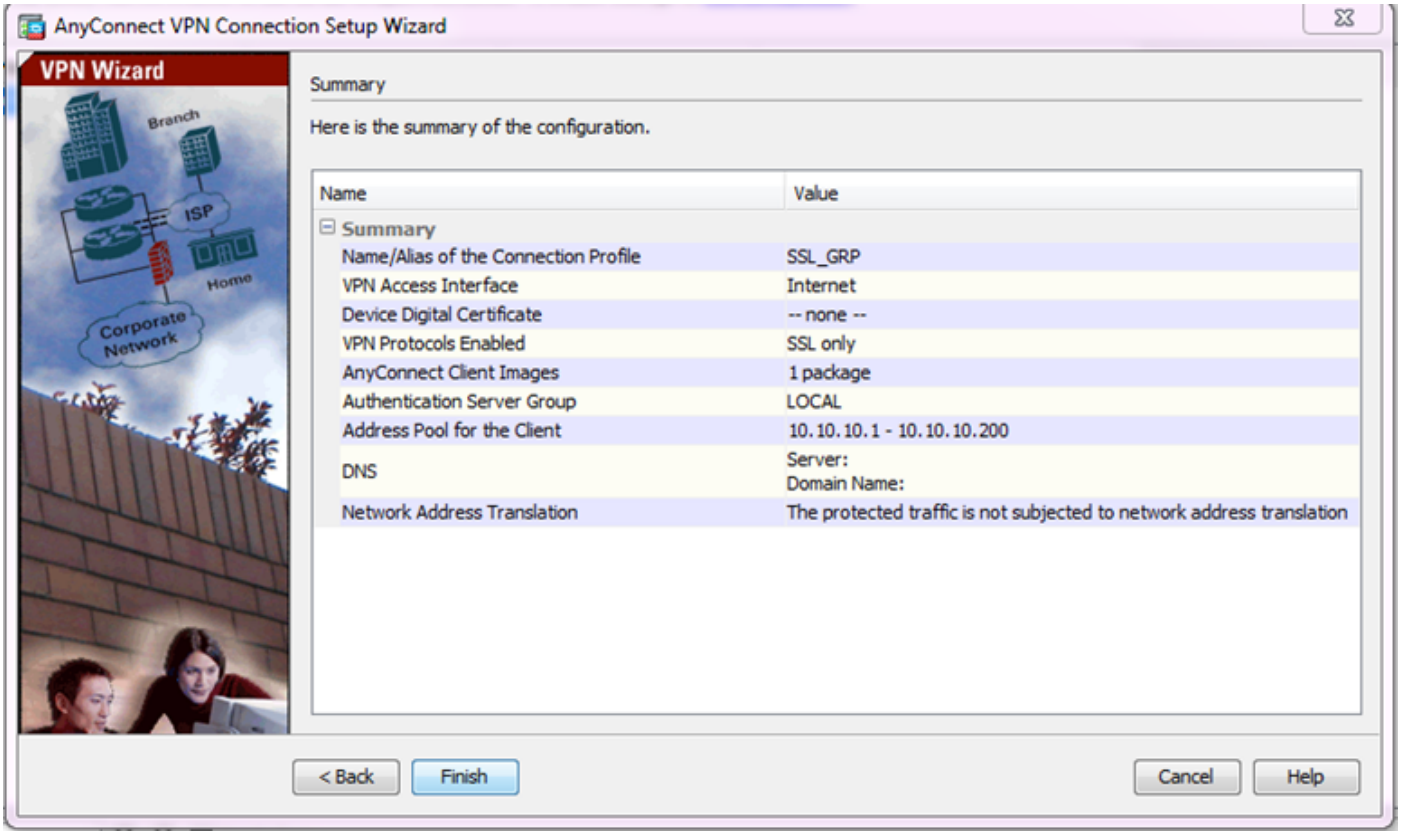
8. Verificare che il traffico tra il client e la subnet interna sia esente da qualsiasi NAT (Network Address Translation) dinamico. Selezionare la casella di controllo Esenzione traffico VPN da conversione indirizzi di rete e configurare l'interfaccia LAN che verrà utilizzata per l'esenzione. Inoltre, specificare la rete locale per la quale si desidera ottenere l'esenzione e fare clic su Avanti.



9. Fare clic su Avanti.



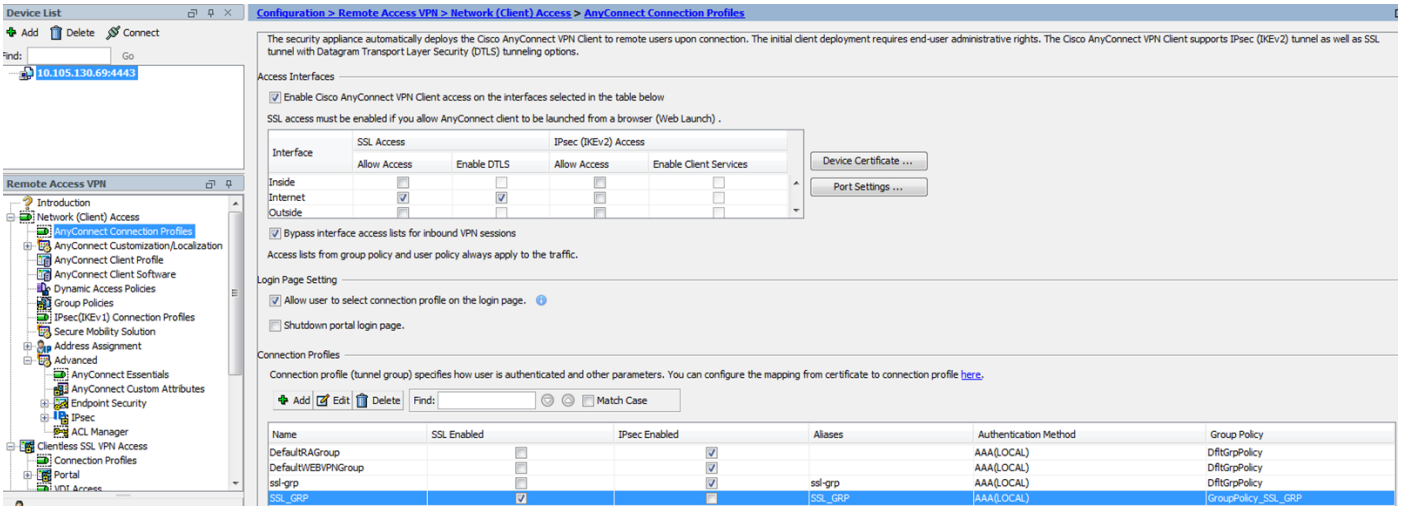
10. L'ultimo passo mostra il riepilogo. Fare clic su Fine per completare l'impostazione.



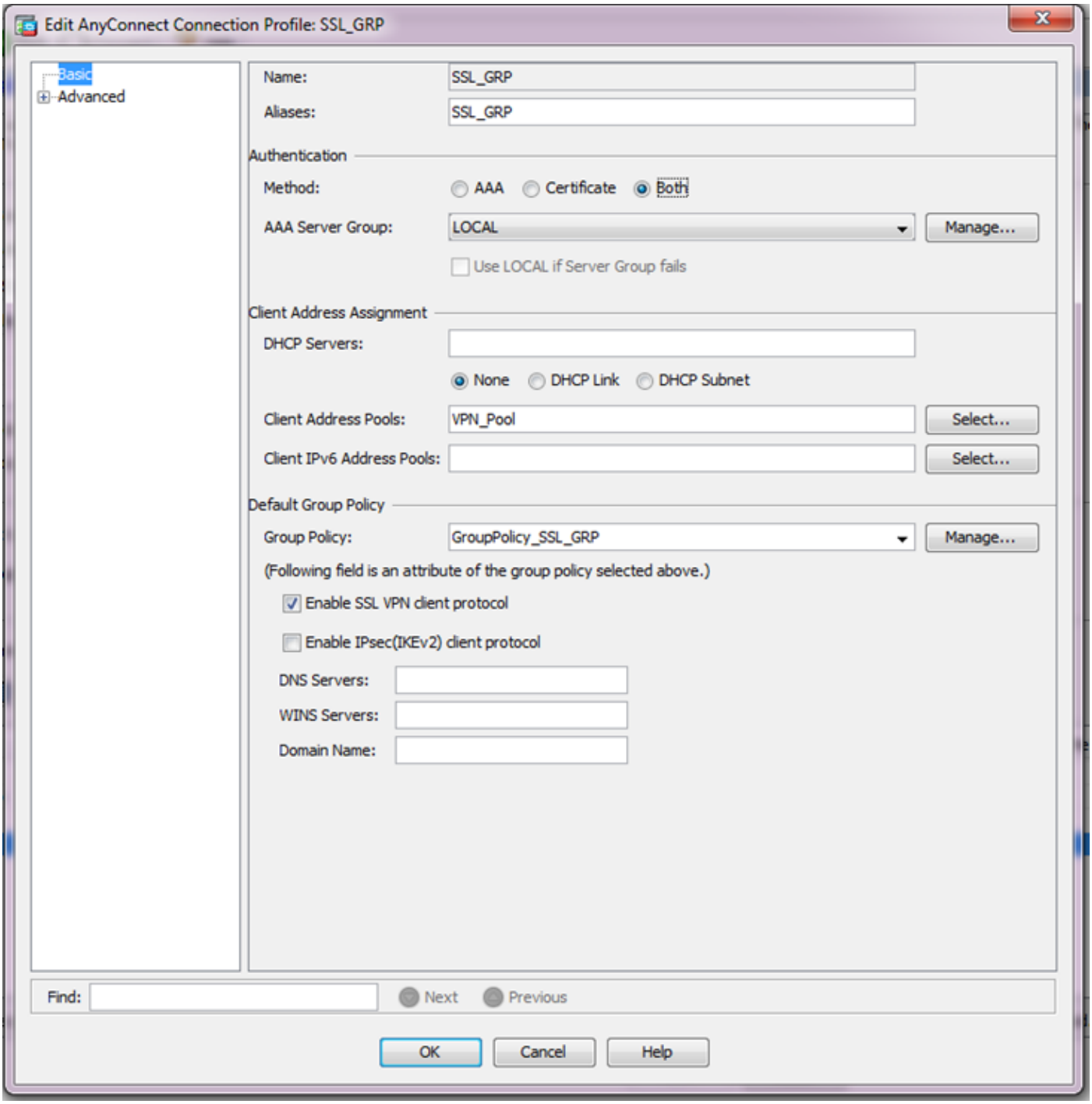
La configurazione del client AnyConnect è ora completata. Tuttavia, quando si configura AnyConnect tramite la Configurazione guidata, il metodo di autenticazione viene configurato come AAA per impostazione predefinita. Per autenticare i client tramite certificati e nome utente/password, è necessario configurare il gruppo di tunnel (profilo di connessione) in modo che

utilizzi i certificati e il server AAA come metodo di autenticazione.

- Selezionare Configurazione > VPN ad accesso remoto > Accesso di rete (client) > Profili di connessione AnyConnect.
- Dovrebbe essere visualizzato il nuovo profilo di connessione SSL_GRP aggiunto.



- Per configurare l'autenticazione AAA e il certificato, selezionare il profilo di connessione SSL_GRP e fare clic su Modifica.
- In Metodo di autenticazione selezionare Entrambi.



Configurazione della CLI per AnyConnect

<#root>

```
!! *****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 destinati
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Nota: lo strumento Output Interpreter (solo utenti registrati) supporta alcuni comandi show. Usare lo strumento Output Interpreter per visualizzare un'analisi dell'output del comando show.

Verificare che il server CA sia abilitato.

show crypto ca server

<#root>

```
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!!
```

Verificare che l'utente sia autorizzato per la registrazione dopo l'aggiunta di:

<#root>

```
*****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
```

È possibile controllare i dettagli della connessione anyconnect tramite CLI o ASDM.

Tramite CLI

show vpn-sessiondb detail anyconnect

<#root>

```
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 :
```

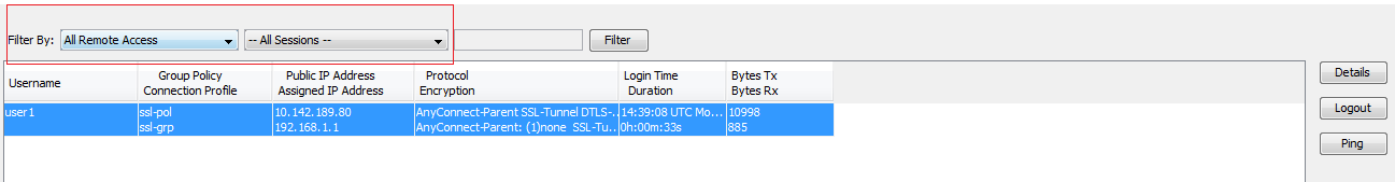
Tramite ASDM

- Passare a Monitoraggio > VPN > Statistiche VPN > Sessioni.
- Scegliere Filtra per come Tutti gli accessi remoti.
- È possibile eseguire una delle azioni elencate di seguito per il client AnyConnect selezionato.

Dettagli: fornire ulteriori informazioni sulla sessione

Disconnessione: per disconnettersi manualmente dall'headend

Ping- Per eseguire il ping del client AnyConnect dall'headend



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

> Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di debug.

> Attenzione: sull'appliance ASA, è possibile impostare vari livelli di debug; per impostazione predefinita, viene usato il livello 1. Se si modifica il livello di debug, il livello di dettaglio dei debug potrebbe aumentare. Procedere con cautela, soprattutto negli ambienti di produzione.

- debug crypto ca
- debug crypto ca server
- debug messaggi ca crittografica
- debug transazioni ca crittografica
- debug webvpn anyconnect

Questo output del comando debug visualizza quando il server CA è abilitato con il comando no shut.

<#root>

```
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!
```

Questo output di debug visualizza la registrazione del client

<#root>

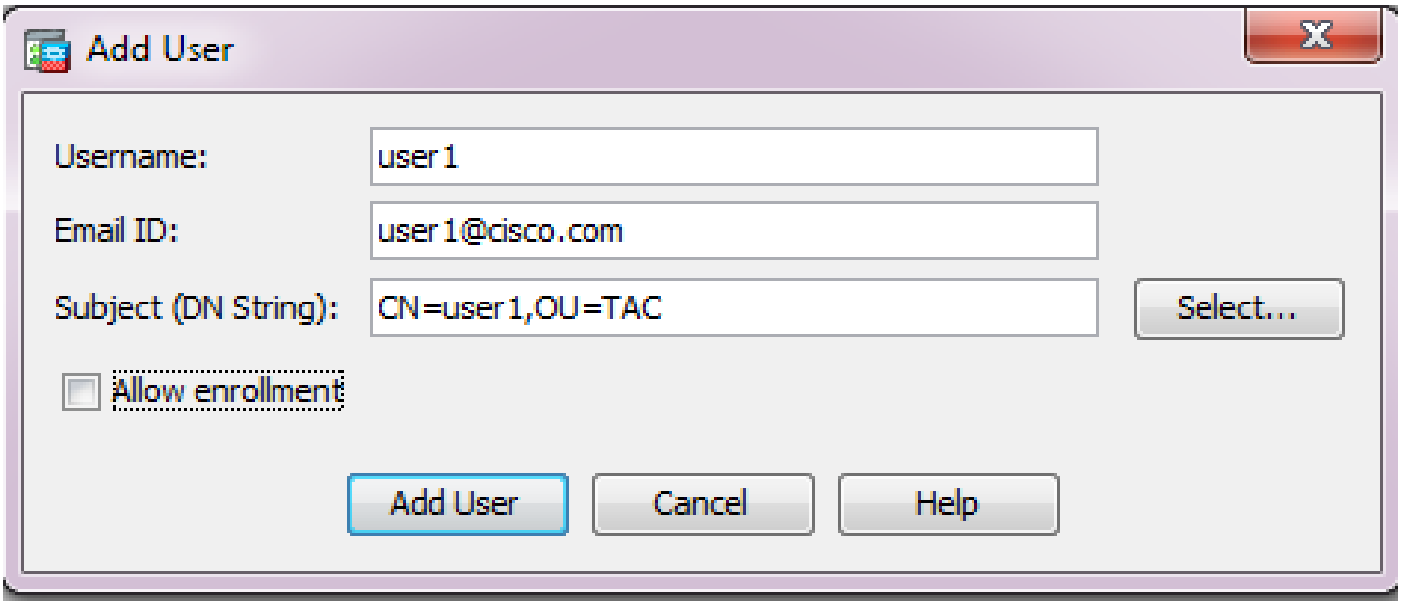
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
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
```

L'iscrizione del client potrebbe non riuscire nelle seguenti condizioni:

Scenario 1.

- L'utente viene creato nel database del server CA senza l'autorizzazione per la registrazione.



Equivalente a CLI:

<#root>

```
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
```

- Nel caso in cui all'utente non sia consentito effettuare la registrazione, il tentativo di generare o inviare tramite e-mail l'OTP per l'utente genera questo messaggio di errore.

Scenario 2.

- Verificare la porta e l'interfaccia su cui è disponibile il portale di registrazione utilizzando il comando show run webvpn. La porta predefinita è 443, ma è possibile modificarla.

- Verificare che il client sia raggiungibile in rete dall'indirizzo IP dell'interfaccia su cui è abilitato webvpn sulla porta utilizzata per accedere correttamente al portale di registrazione.

Il client potrebbe non riuscire ad accedere al portale di registrazione dell'ASA nei seguenti casi:

1. Se un dispositivo intermedio blocca le connessioni in arrivo dal client all'IP webvpn dell'ASA sulla porta specificata.
2. Lo stato dell'interfaccia non è attivo su cui webvpn è abilitato.

- Questo output mostra che il portale di registrazione è disponibile all'indirizzo IP dell'interfaccia Internet sulla porta personalizzata 4433.

<#root>

```
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
```

Scenario 3.

- La posizione predefinita di Archiviazione database del server CA è la memoria flash dell'appliance ASA.
- Verificare che la memoria flash disponga di spazio libero per generare e salvare il file pkcs12 per l'utente durante la registrazione.
- Se la memoria flash non dispone di spazio libero sufficiente, l'ASA non riesce a completare il processo di registrazione del client e genera i seguenti log di debug:

<#root>

```
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
```

Informazioni correlate

- Cisco ASA serie 5500 Adaptive Security Appliance
- Guida alla risoluzione dei problemi dei client VPN AnyConnect - Problemi comuni
- Gestione, monitoraggio e risoluzione dei problemi delle sessioni AnyConnect
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).