ASA als lokalen CA-Server und AnyConnect-Headend konfigurieren

Inhalt

Einleitung

In diesem Dokument wird die Einrichtung einer Cisco Adaptive Security Appliance (ASA) als CA-Server (Certificate Authority) und SSL-Gateway (Secure Sockets Layer) für Cisco AnyConnect Secure Mobility Clients beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende ASA-Konfiguration mit Softwareversion 9.1.x
- ASDM 7.3 oder höher

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

- Cisco ASA 5500 Serie mit Software-Version 9.1(6)
- AnyConnect Secure Mobility Client Version 4.x für Windows
- PC, auf dem ein gemäß der Kompatibilitätstabelle unterstütztes Betriebssystem ausgeführt wird.
- Cisco Adaptive Security Device Manager (ASDM) Version 7.3

Hinweis: Laden Sie das AnyConnect VPN Client-Paket (anyconnect-win*.pkg) aus dem Cisco Software-Download herunter (nur für registrierte Kunden). Kopieren Sie den AnyConnect VPN Client in den Flash-Speicher der ASA. Er muss auf die Remote-Benutzercomputer heruntergeladen werden, damit die SSL-VPN-Verbindung mit der ASA hergestellt werden kann. Weitere Informationen finden Sie im Abschnitt Installing the AnyConnect Client (Installieren des AnyConnect-Clients) im ASA-Konfigurationsleitfaden.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

Die Zertifizierungsstelle der ASA stellt folgende Funktionen bereit:

- Integration des grundlegenden Zertifizierungsstellenbetriebs in die ASA.
- Stellt Zertifikate bereit.
- Bietet eine sichere Sperrprüfung ausgestellter Zertifikate.
- Bietet eine Zertifizierungsstelle auf der ASA zur Verwendung mit browserbasierten (WebVPN) und clientbasierten (AnyConnect) SSL VPN-Verbindungen.
- Stellt Benutzern vertrauenswürdige digitale Zertifikate zur Verfügung, ohne dass externe Zertifikatautorisierung erforderlich ist.
- Bietet eine sichere, interne Autorität für die Zertifikatsauthentifizierung und ermöglicht die unkomplizierte Benutzerregistrierung mittels Website-Login.

Richtlinien und Einschränkungen

- Wird im Routing- und transparenten Firewall-Modus unterstützt.
- Auf einer ASA kann jeweils nur ein lokaler CA-Server vorhanden sein.
- ASA als lokaler CA-Server wird in einer Failover-Konfiguration nicht unterstützt.
- Die ASA, die derzeit als lokaler Zertifizierungsstellenserver fungiert, unterstützt nur die Generierung von SHA1-Zertifikaten.
- Der lokale CA-Server kann für browser- und clientbasierte SSL VPN-Verbindungen verwendet werden. Derzeit nicht unterstützt für IPSec.
- Keine Unterstützung für VPN-Lastenausgleich für die lokale Zertifizierungsstelle.
- Die lokale Zertifizierungsstelle darf keiner anderen Zertifizierungsstelle untergeordnet sein.

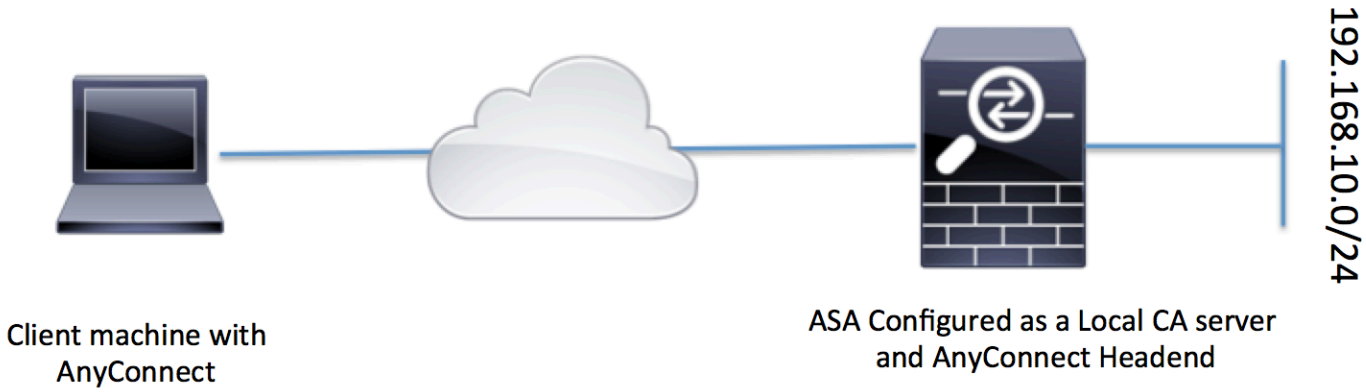
Sie kann nur als Stammzertifizierungsstelle fungieren.
- Derzeit kann sich die ASA nicht beim lokalen CA-Server für das Identitätszertifikat anmelden.
- Nach Abschluss der Zertifikatsregistrierung speichert die ASA eine PKCS12-Datei mit der Tastatur und der Zertifikatskette des Benutzers, die pro Registrierung etwa 2 KB Flash-Speicher oder Speicherplatz benötigt. Der tatsächliche Speicherplatz hängt von der konfigurierten RSA-Schlüsselgröße und den Zertifikatfeldern ab. Beachten Sie diese Richtlinie, wenn Sie eine große Anzahl ausstehender Zertifikatregistrierungen auf einem ASA-Gerät mit einem begrenzten verfügbaren Flash-Speicher hinzufügen, da diese PKCS12-Dateien während des konfigurierten Zeitlimits für den Registrierungsabruf im Flash-Speicher gespeichert werden.

Konfigurieren

In diesem Abschnitt wird beschrieben, wie die Cisco ASA als lokaler Zertifizierungsstellenserver konfiguriert wird.

Hinweis: Verwenden Sie das Command Lookup Tool, also das Tool für die Suche nach Befehlen (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm



ASA als lokaler Zertifizierungsstellenserver

Schritt 1: Konfiguration und Aktivierung des lokalen Zertifizierungsstellenservers auf der ASA

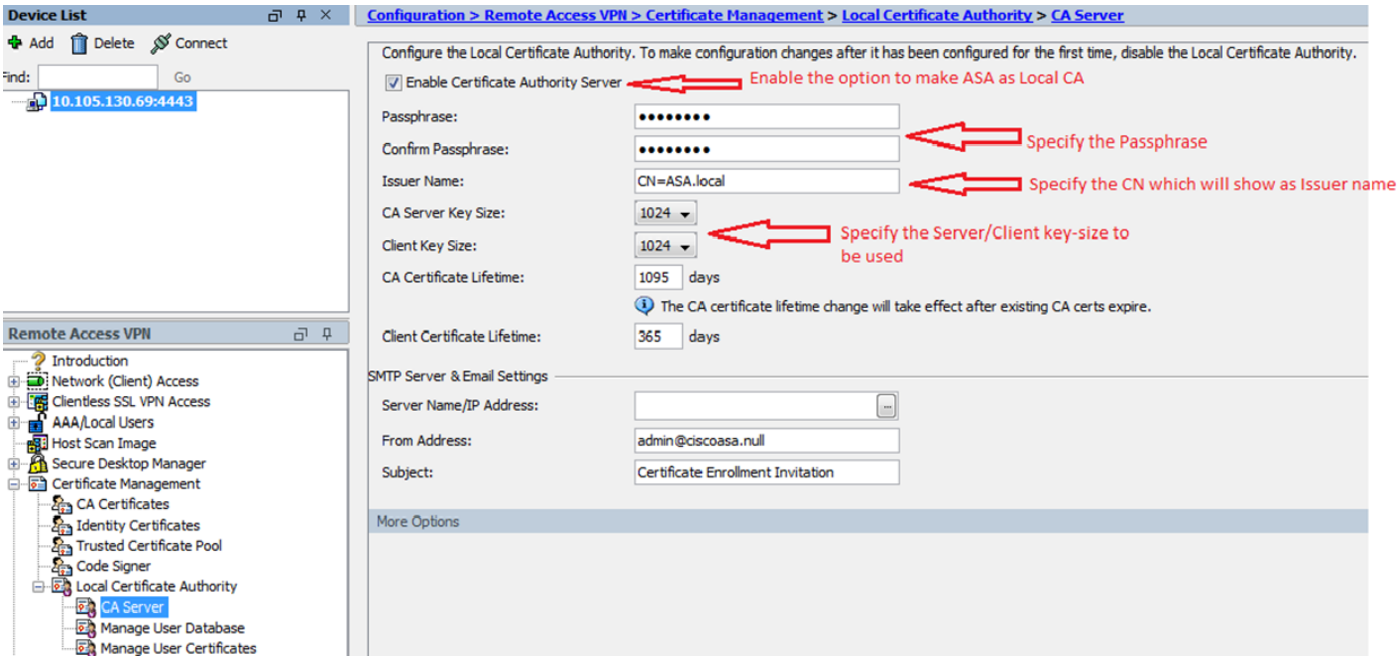
- Navigieren Sie zu Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server. Aktivieren Sie die Option Zertifizierungsstellen-Server aktivieren.

- Konfigurieren der Passphrase Die Passphrase muss mindestens 7 Zeichen lang sein und zum Codieren und Speichern einer PKCS12-Datei mit dem lokalen CA-Zertifikat und dem Schlüsselpaar verwendet werden. Die Passphrase entsperrt das PKCS12-Archiv, wenn das Zertifizierungsstellenzertifikat oder das Schlüsselpaar verloren geht.

- Konfigurieren Sie den Namen des Ausstellers. Dieses Feld wird als Stammzertifikat-CN angezeigt. Dies kann im folgenden Format angegeben werden: CN (Common Name), OU (Organisationseinheit), (O) Organisation , L (Lokalität) , S (Staat) und C (Land).

- Optionale Konfiguration: Konfigurieren Sie die Einstellungen für den SMTP-Server und den E-Mail-Server, um sicherzustellen, dass das OTP zum Abschluss der Registrierung per E-Mail an die Endkunden empfangen werden kann. Sie können den Hostnamen oder die IP-Adresse Ihres lokalen E-Mail-/SMTP-Servers konfigurieren. Sie können auch die Absenderadresse und das Betreff-Feld der E-Mail konfigurieren, die die Clients empfangen sollen. Standardmäßig lautet die Absenderadresse admin@<ASA-Hostname>.null, und der Betreff lautet Zertifikatregistrierungseinladung.

- Optionale Konfiguration: Sie können die optionalen Parameter wie Clientschlüsselgröße, Größe des CA-Serverschlüssels, Lebensdauer des CA-Zertifikats und Lebensdauer des Clientzertifikats ebenfalls konfigurieren.



CLI-Äquivalent:

```
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
```

Dies sind zusätzliche Felder, die unter Konfiguration des lokalen Zertifizierungsstellenservers konfiguriert werden können.

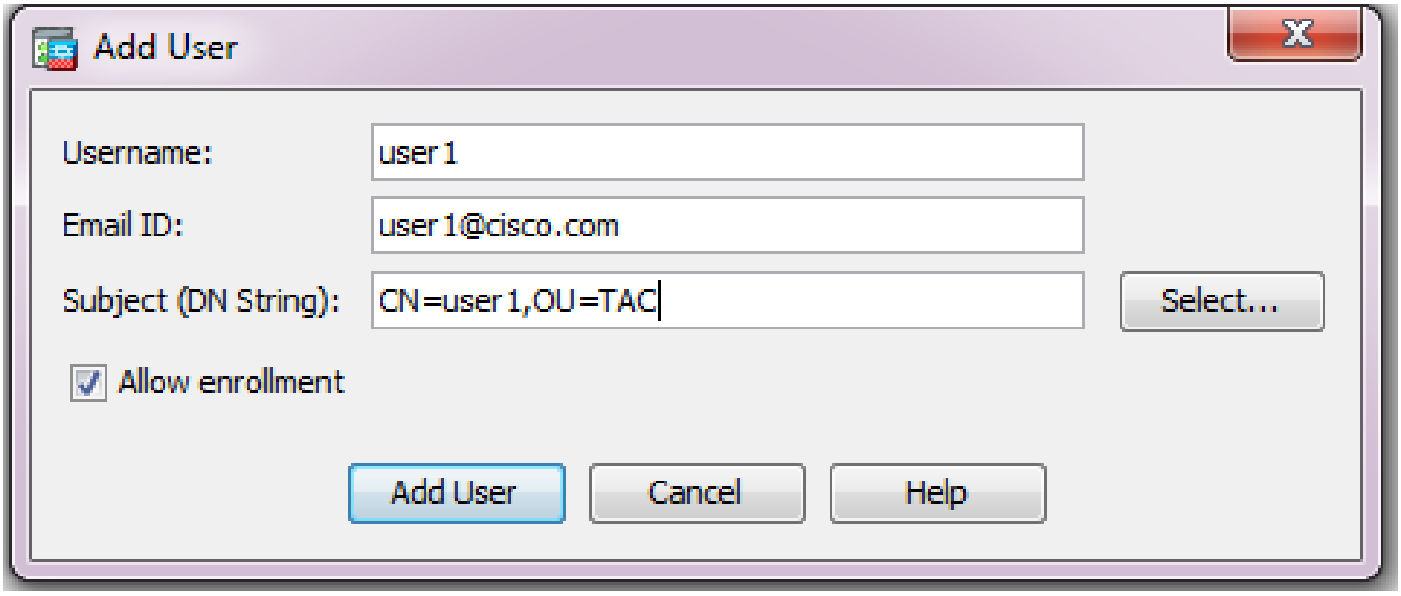
URL des CRL-Verteilungspunkts	Dies ist der Zertifikatsperrlisten-Standort auf der ASA. Der Standardspeicherort ist http://hostname.domain/+CSCOCA+/asa_ca.crl, aber die URL kann geändert werden.
Publishing-CRL-Schnittstelle und -Port	Um die Zertifikatsperrliste für den HTTP-Download auf einer bestimmten Schnittstelle und einem bestimmten Port verfügbar zu machen, wählen Sie in der Dropdown-Liste eine Schnittstelle für die Veröffentlichung aus. Geben Sie dann die Portnummer ein. Dabei kann es sich um eine beliebige Portnummer zwischen 1 und 65535 handeln. Die Standard-Portnummer lautet TCP-Port 80.
Lebensdauer der Sperrliste	Die lokale Zertifizierungsstelle aktualisiert und gibt die Zertifikatsperrliste jedes Mal neu aus, wenn ein Benutzerzertifikat widerrufen oder nicht widerrufen wird. Wenn jedoch keine Widerrufsänderungen vorgenommen werden, wird die Zertifikatsperrliste automatisch erneut ausgestellt, sobald die Lebensdauer der Zertifikatsperrliste erreicht ist. Dies ist der Zeitraum, den Sie mit dem Befehl lifetime crlcommand während der Konfiguration der lokalen Zertifizierungsstelle angeben. Wenn Sie keine Lebensdauer der Zertifikatsperrliste angeben, beträgt der Standardzeitraum sechs Stunden.
Speicherort des Datenbankspeichers	Die ASA greift mithilfe einer lokalen Zertifizierungsstellendatenbank auf Benutzerinformationen, ausgestellte Zertifikate und Sperrlisten zu und implementiert diese. Diese Datenbank befindet sich standardmäßig im lokalen Flash-Speicher oder kann für ein externes Dateisystem konfiguriert werden, das bereitgestellt wird und auf das ASA zugreifen kann.
Standardbetreff-Name	Geben Sie einen Standardbetreff (DN-Zeichenfolge) ein, der an einen Benutzernamen auf ausgestellten Zertifikaten angehängt werden soll. Die zulässigen DN-Attribute werden in der folgenden Liste bereitgestellt: · CN (Common Name)SN (Name) · O (Name der Organisation)

	· L (Ort) · C (Land) · OU (Organisationseinheit) · EA (E-Mail-Adresse) · ST (Bundesland) · T (Titel)
Registrierungszeitraum	Legt die Registrierungsfrist in Stunden fest, innerhalb derer der Benutzer die PKCS12-Datei von der ASA abrufen kann. Der Standardwert ist 24 Stunden. **Hinweis:** Wenn der Registrierungszeitraum abläuft, bevor der Benutzer die PKCS12-Datei abruft, die das Benutzerzertifikat enthält, ist die Registrierung nicht zulässig.
Einmaliges Kennwortablauf	Definiert den Zeitraum in Stunden, für den das OTP für die Benutzerregistrierung gültig ist. Dieser Zeitraum beginnt, wenn der Benutzer sich registrieren darf. Der Standardwert ist 72 Stunden.
Erinnerung zum Ablauf des Zertifikats	Gibt die Anzahl der Tage vor Ablauf des Zertifikats an, die eine erste Erinnerung zur erneuten Anmeldung an die Zertifikatbesitzer gesendet wird.

Schritt 2: Erstellen und Hinzufügen von Benutzern zur ASA-Datenbank

- Navigieren Sie zu Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database.Klicken Sie auf Add.

- Geben Sie die Benutzerdetails an, z. B. Benutzername, E-Mail-ID und den Betreffnamen, wie in diesem Bild dargestellt.



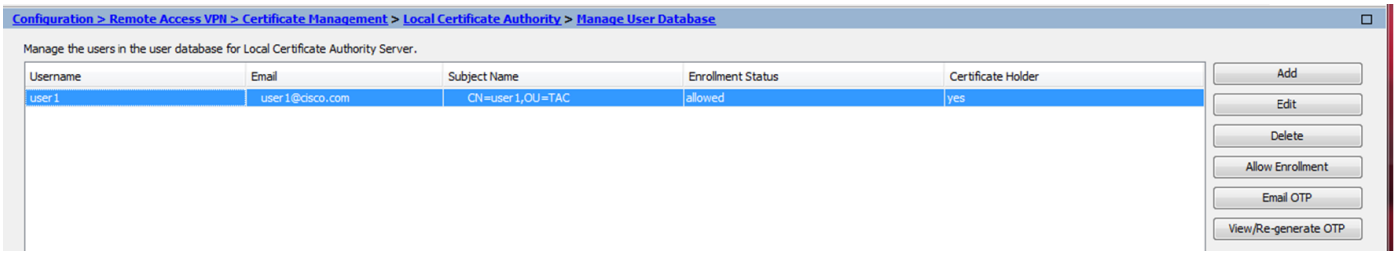
- Stellen Sie sicher, dass die Option Anmeldung zulassen aktiviert ist, damit Sie sich für das Zertifikat registrieren können.
- Klicken Sie auf Benutzer hinzufügen, um die Benutzerkonfiguration abzuschließen.

CLI-Äquivalent:

<#root>

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

- Nachdem der Benutzer zur Benutzerdatenbank hinzugefügt wurde, wird der Registrierungsstatus als Zulässig für die Registrierung angezeigt.



CLI zum Überprüfen des Benutzerstatus:

<#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:
```

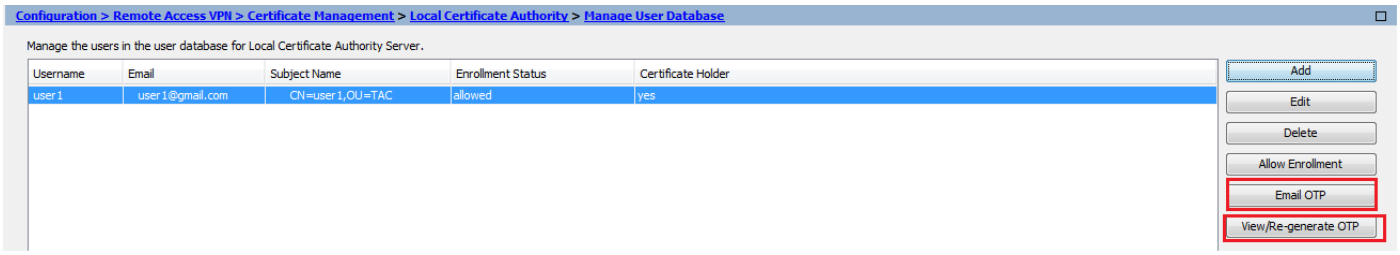
Allowed to Enroll

- Nachdem der Benutzer zur Benutzerdatenbank hinzugefügt wurde, kann das einmalige Kennwort (One Time Password, OTP) für den Benutzer zum Abschluss der Registrierung folgendermaßen bereitgestellt werden:

Senden Sie eine E-Mail an das OTP (SMTP-Server und E-Mail-Einstellungen müssen unter der Konfiguration des CA-Servers konfiguriert sein).

ODER

Sie können das OTP direkt anzeigen und für den Benutzer freigeben, indem Sie auf "OTP anzeigen/neu generieren" klicken. Dies kann auch zum Regenerieren des OTP verwendet werden.



CLI-Äquivalent:

```
!! 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
```

Schritt 3: Aktivieren von WebVPN an der WAN-Schnittstelle

- Aktivieren Sie auf der ASA den Webzugriff, damit Clients eine Registrierung beantragen können.

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

Schritt 4: Zertifikat auf den Client-Computer importieren

- Öffnen Sie auf der Client-Workstation einen Browser, und navigieren Sie zum Link, um die Registrierung abzuschließen.
- Bei dem für diese Verbindung verwendeten IP/FQDN sollte es sich um die IP-Adresse der Schnittstelle handeln, für die in diesem Schritt WebVPN aktiviert ist, d. h. der Schnittstelle Internet.

<#root>

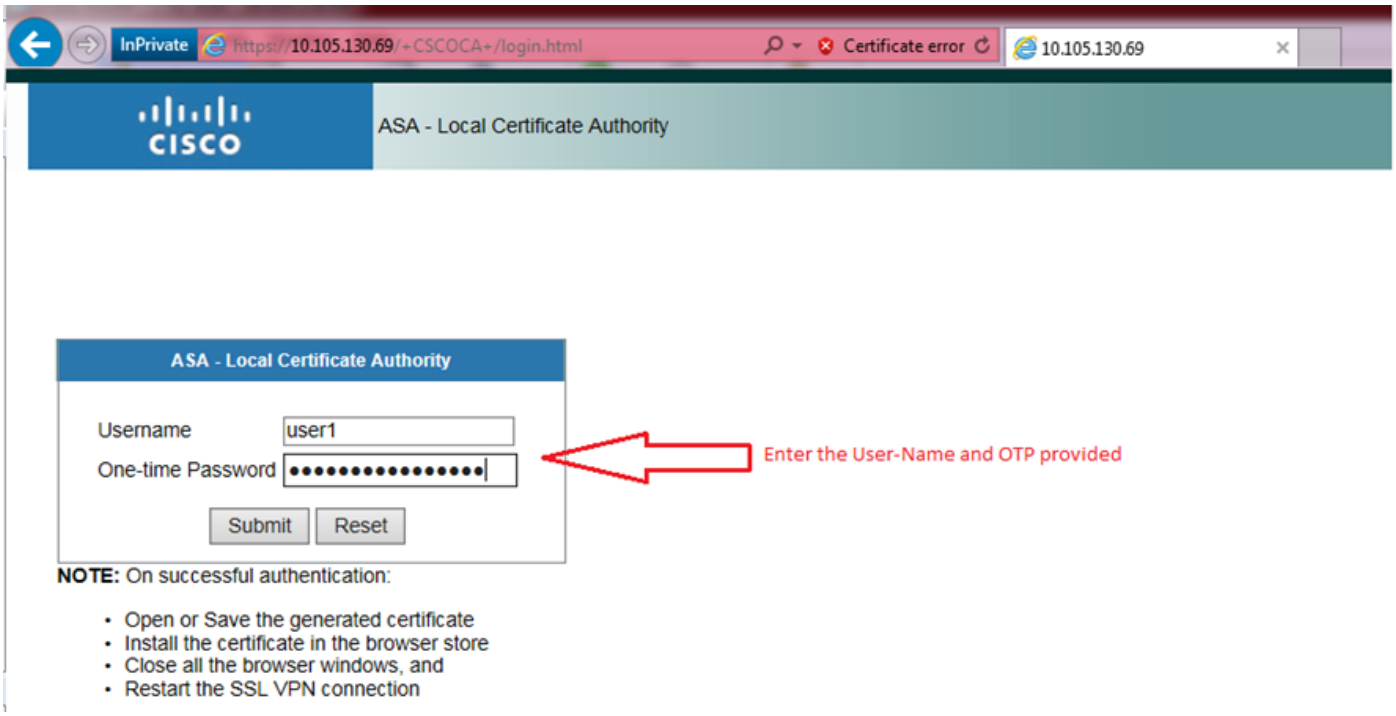
https://

<>

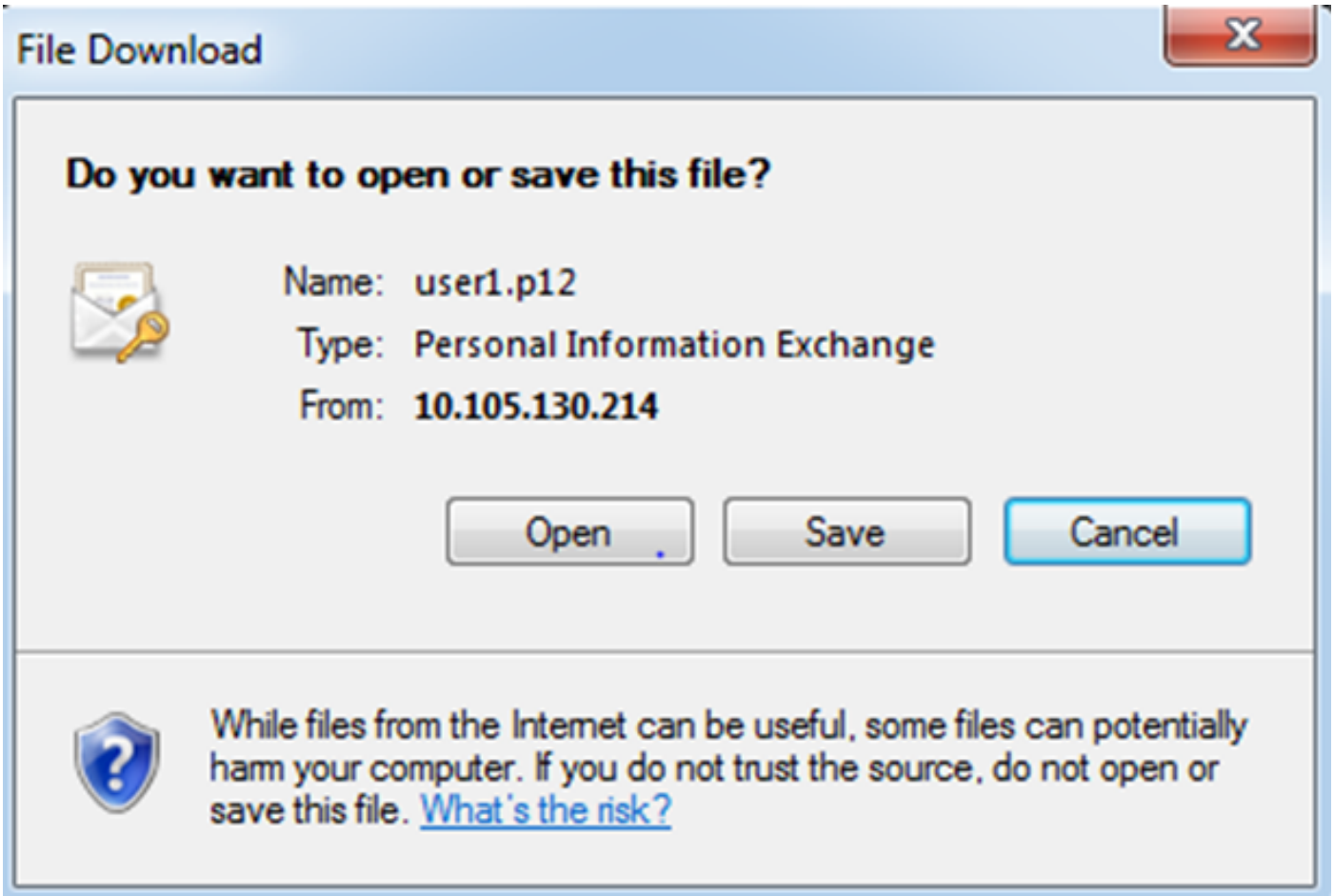
IP/FQDN>/+CSCOCA+/enroll.html

<>

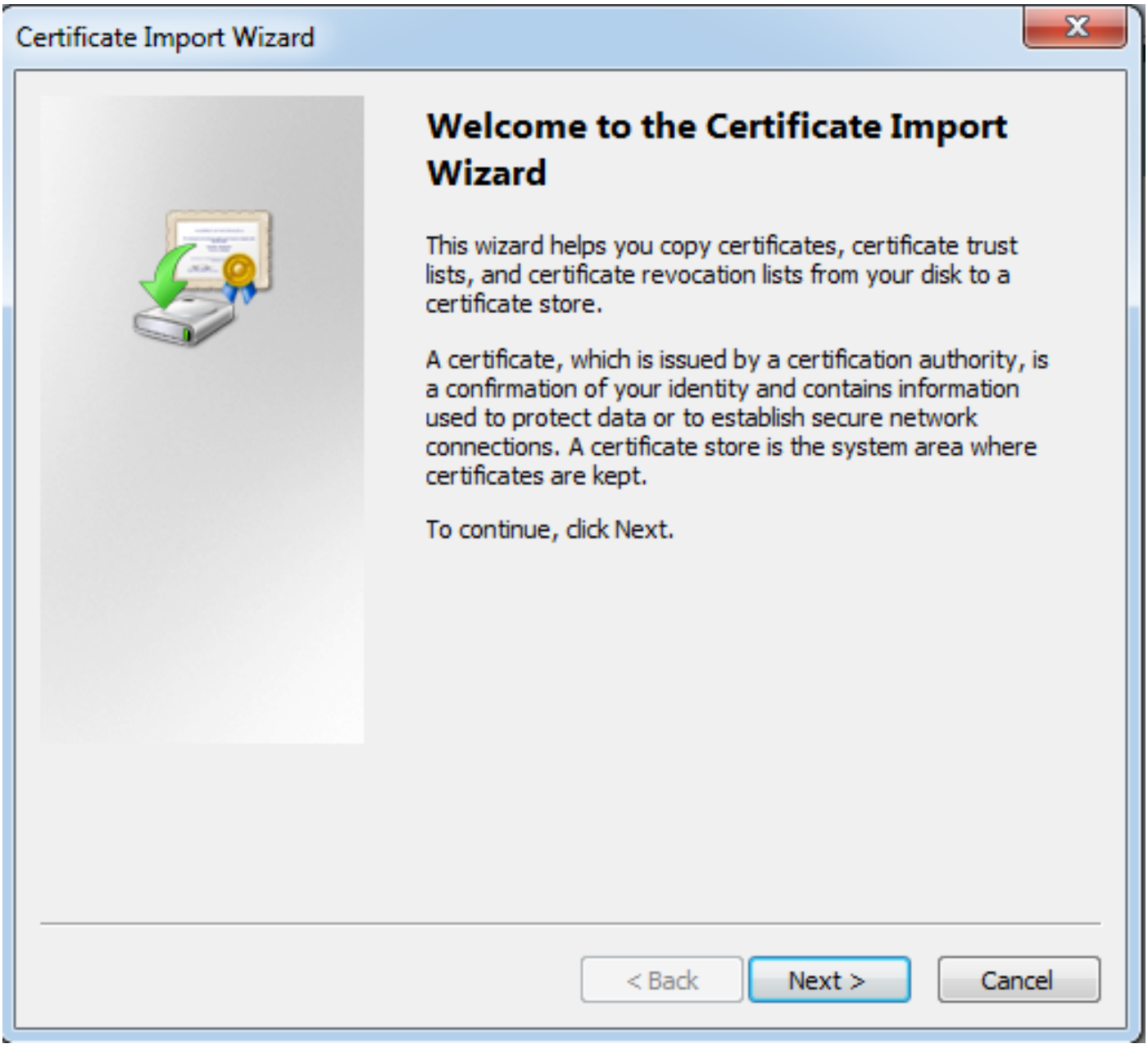
- Geben Sie den Benutzernamen (konfiguriert auf dem ASA unter Schritt 2, Option A) und das OTP ein, das per E-Mail oder manuell bereitgestellt wurde.



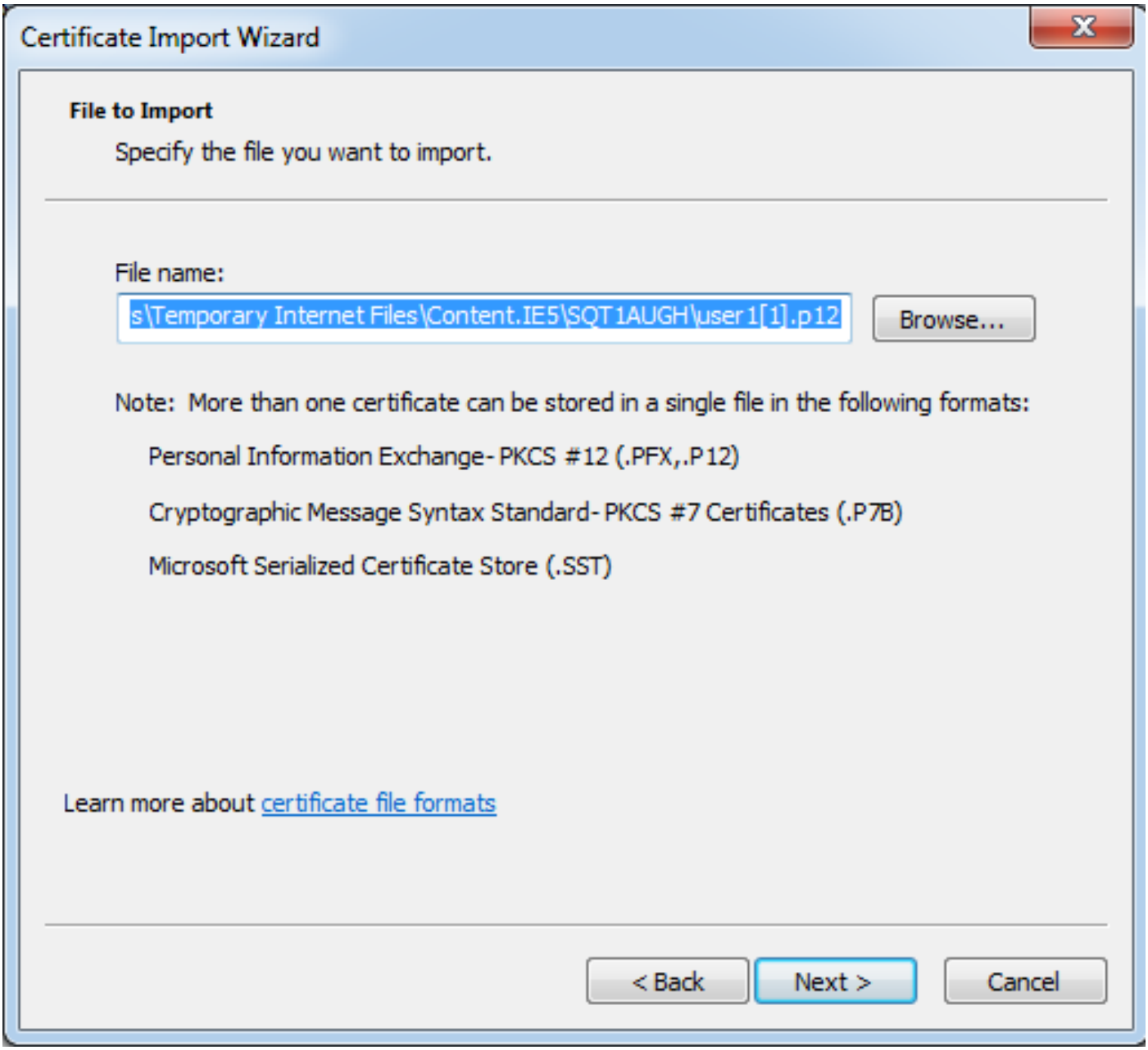
- Klicken Sie auf Öffnen, um das von der ASA erhaltene Client-Zertifikat direkt zu installieren.
- Die Passphrase für die Installation des Client-Zertifikats entspricht dem zuvor empfangenen OTP.



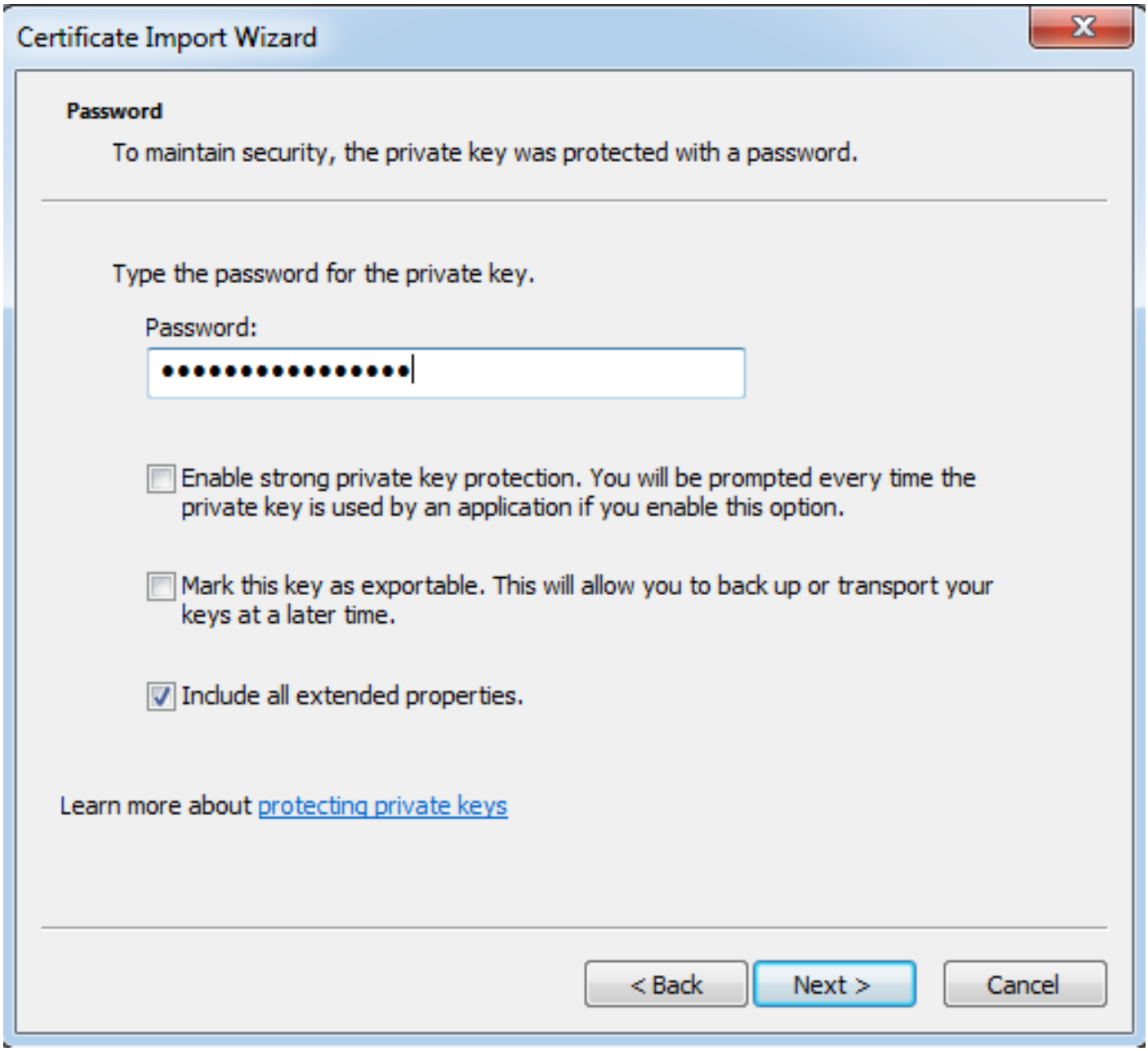
- Klicken Sie auf Next (Weiter).



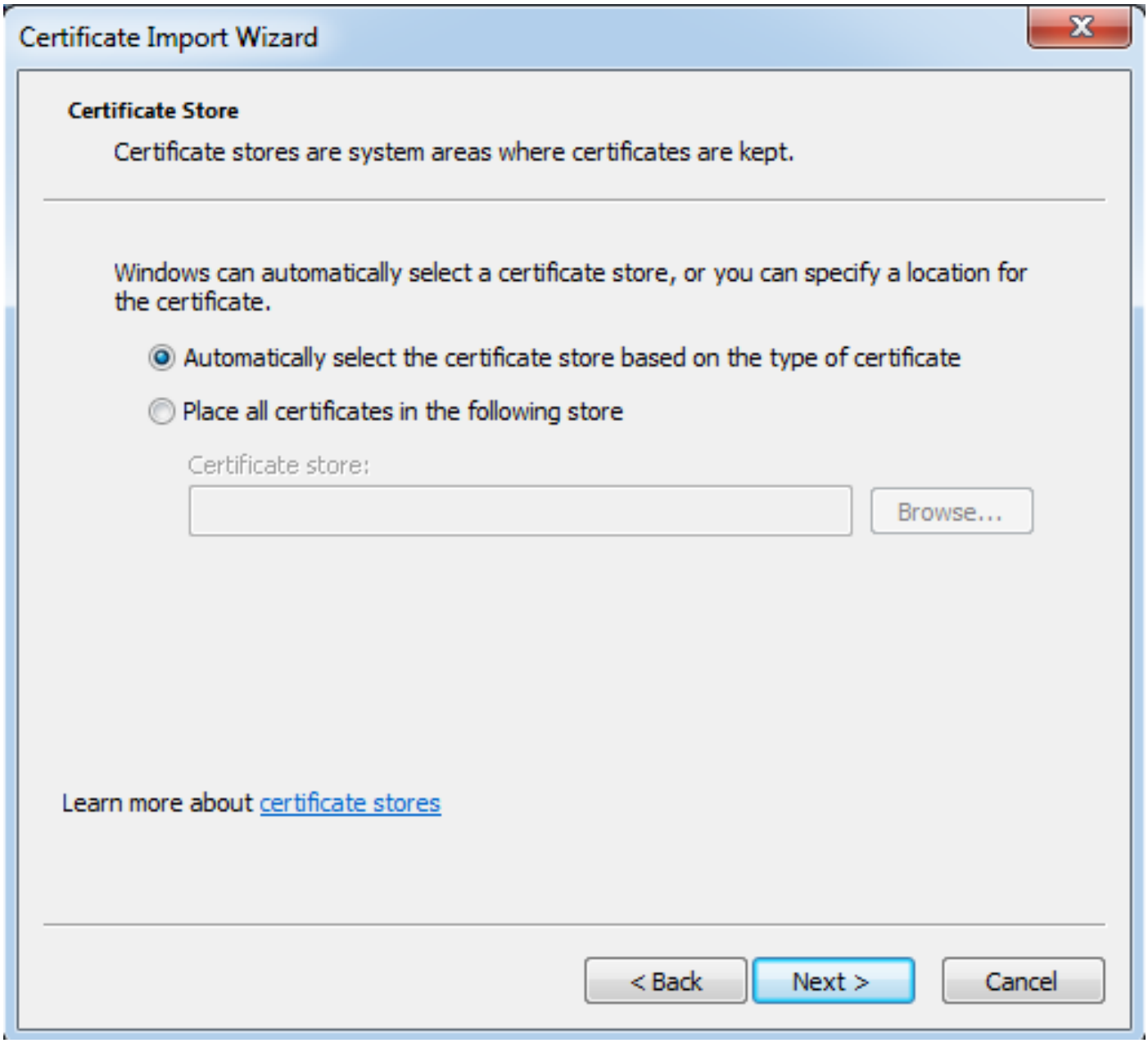
- Behalten Sie den Pfad als Standard bei, und klicken Sie auf Weiter.



- Geben Sie das OTP in das Feld Kennwort ein.
- Sie können die Option auswählen, diesen Schlüssel als exportierbar zu markieren, sodass er bei Bedarf später von der Workstation exportiert werden kann.
- Klicken Sie auf Next (Weiter).



- Sie können das Zertifikat manuell in einem bestimmten Zertifikatspeicher installieren oder den Speicher automatisch auswählen lassen.
- Klicken Sie auf Next (Weiter).



- Klicken Sie auf Fertig stellen, um die Installation abzuschließen.

Certificate Import Wizard

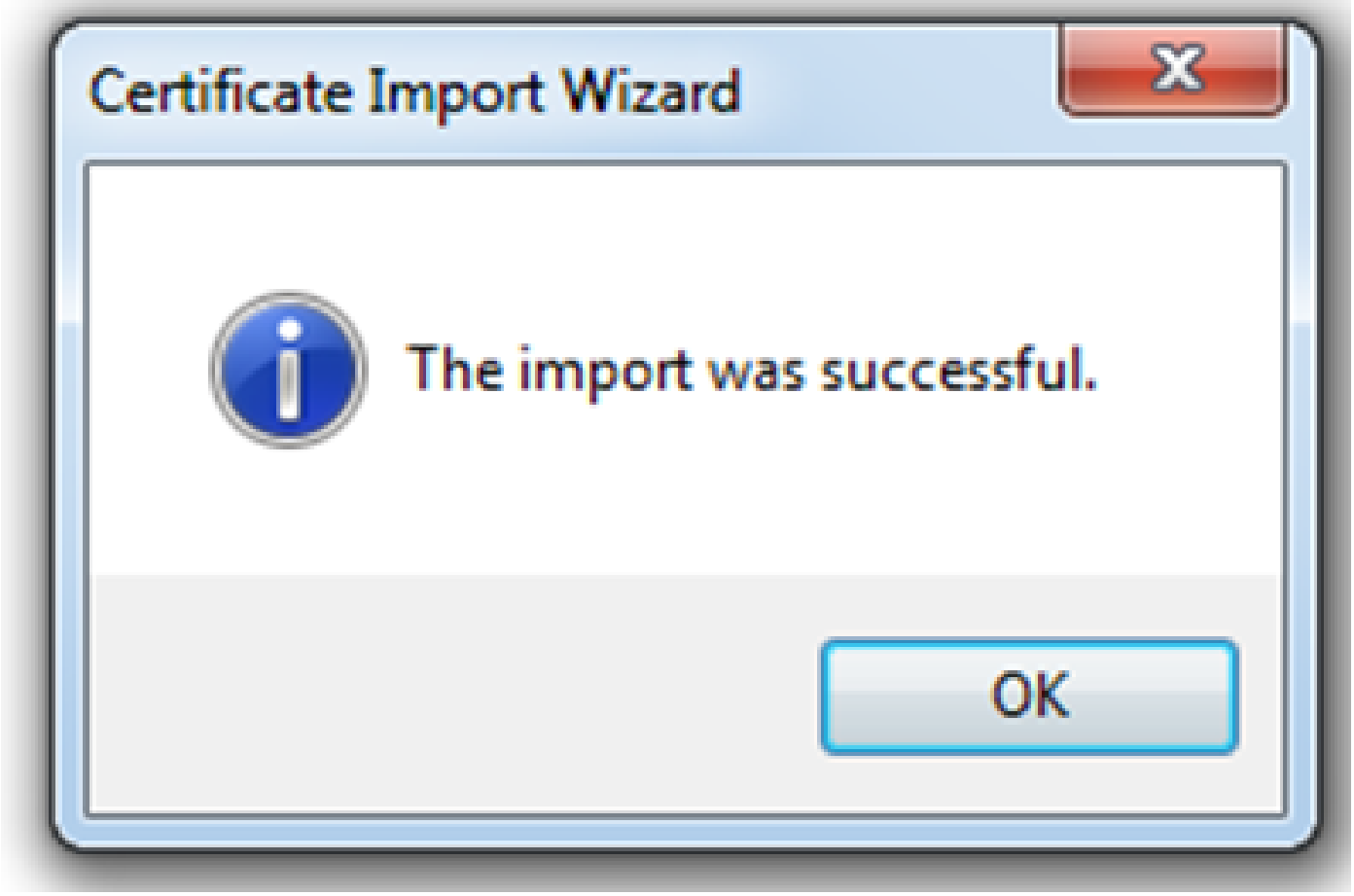
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

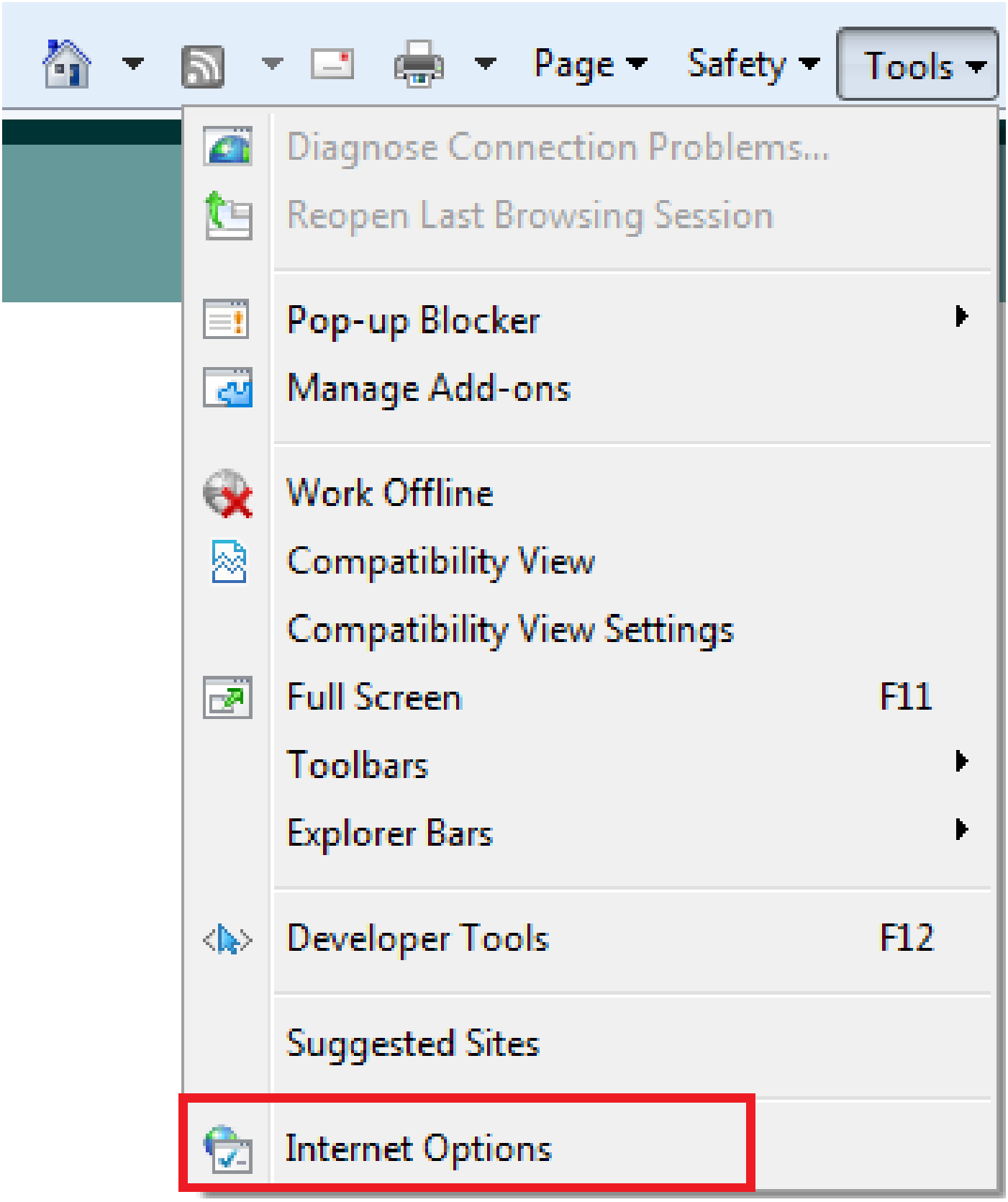
You have specified the following settings:

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

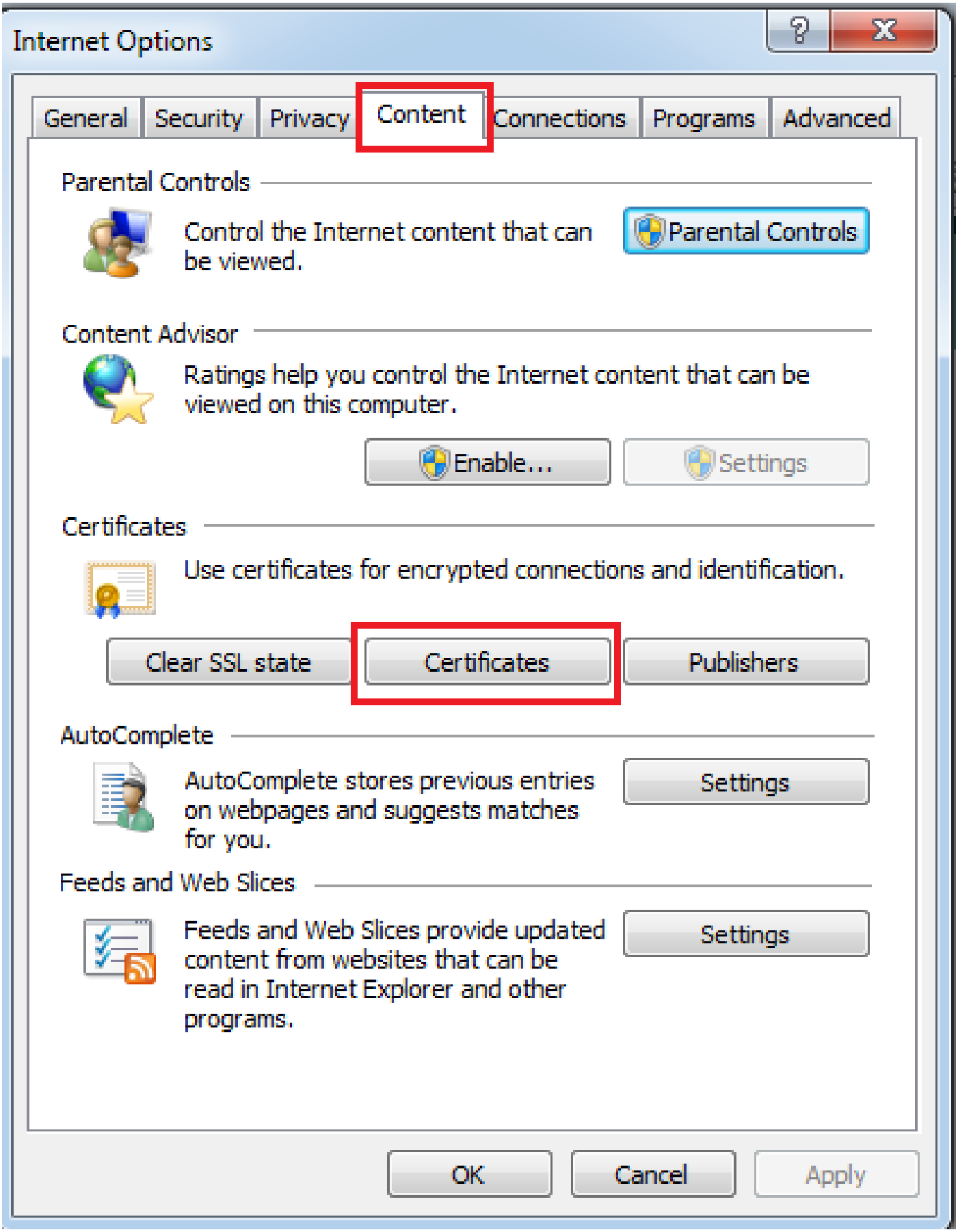
< Back | Finish | Cancel



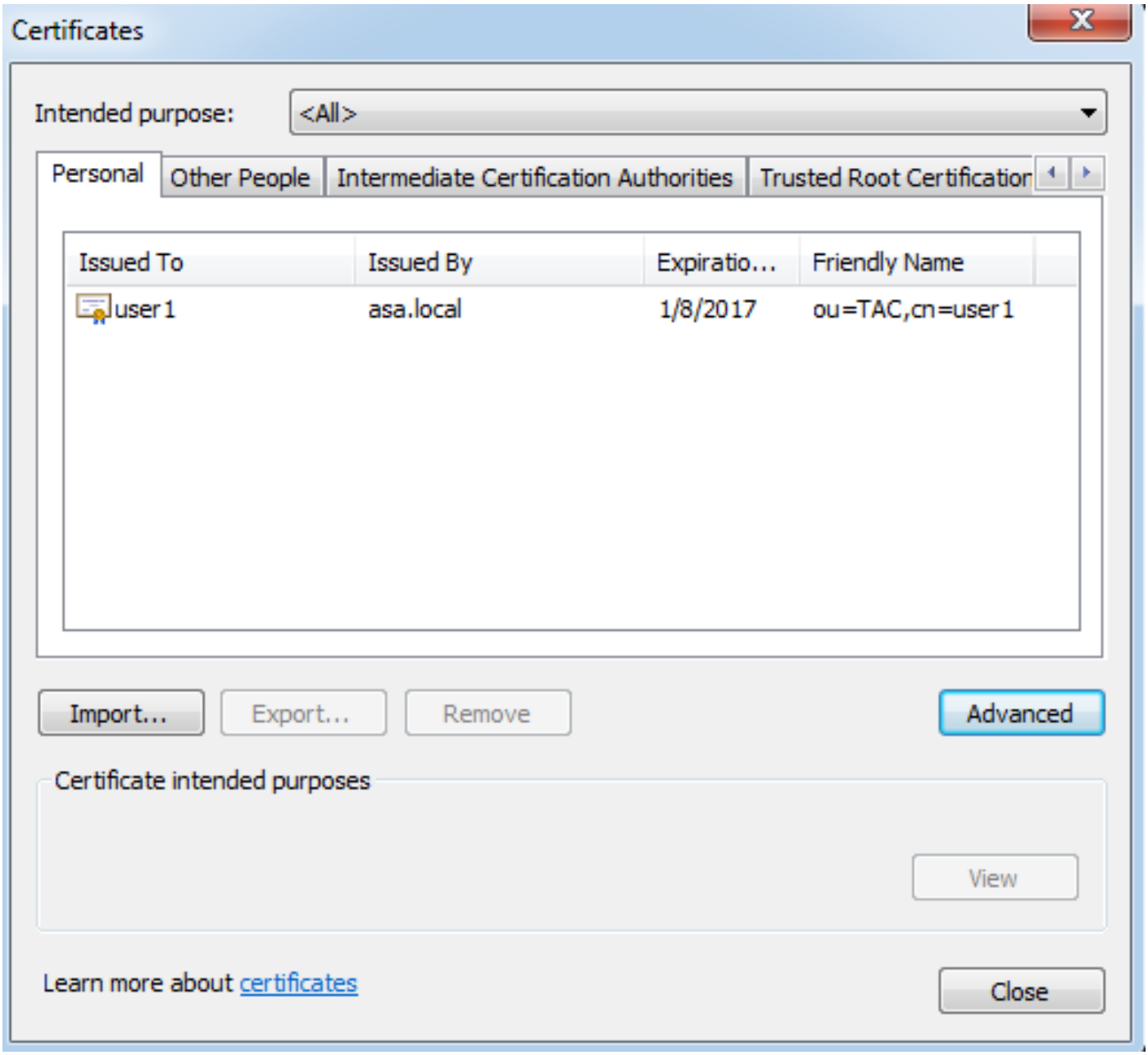
- Sobald das Zertifikat erfolgreich installiert wurde, können Sie es überprüfen.
- Öffnen Sie IE, und navigieren Sie zu Extras > Internetoptionen.



- Navigieren Sie zur Registerkarte Inhalt, und klicken Sie auf Zertifikate, wie in diesem Bild dargestellt.



- Im persönlichen Datenspeicher können Sie das von der ASA empfangene Zertifikat sehen.



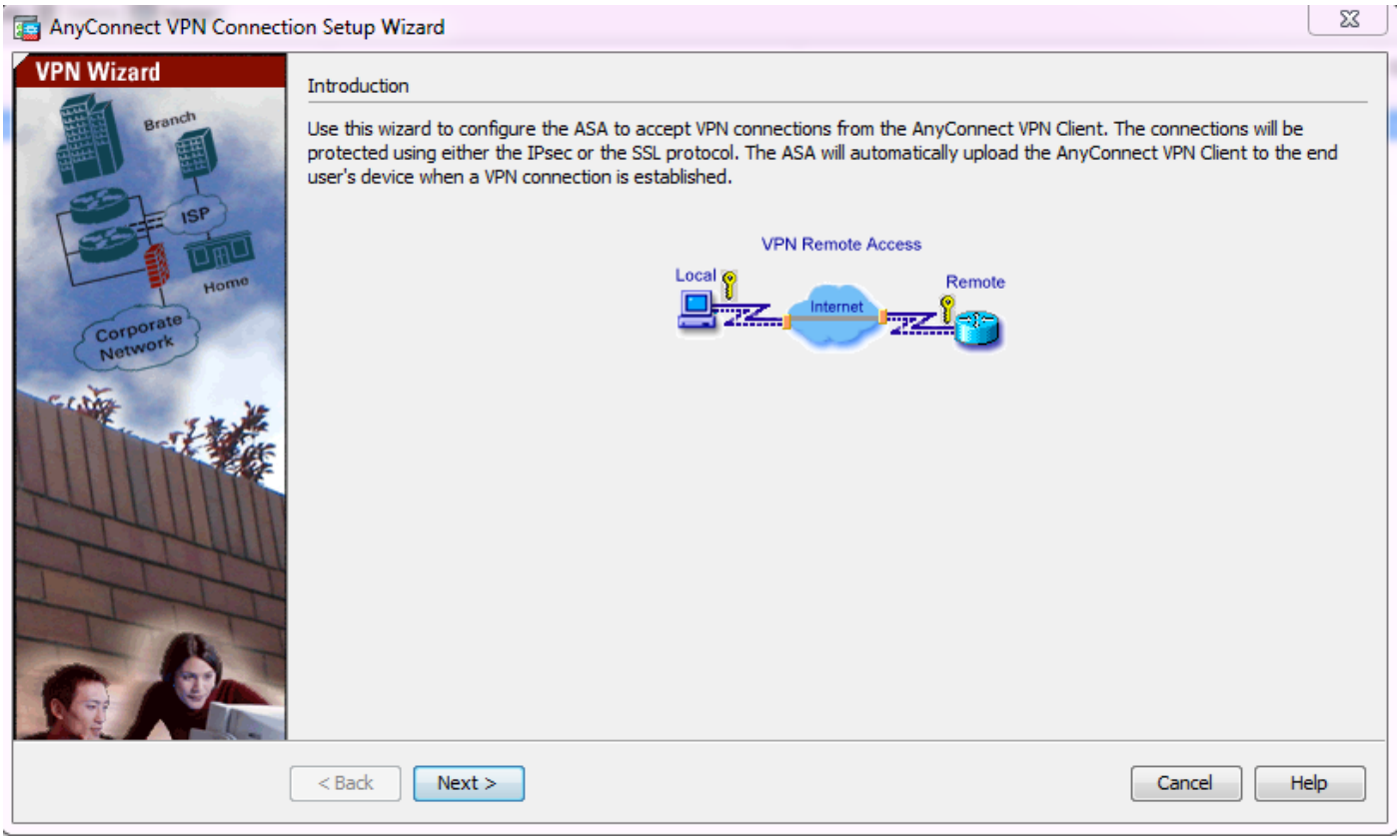
ASA als SSL-Gateway für AnyConnect-Clients

ASDM AnyConnect-Konfigurationsassistent

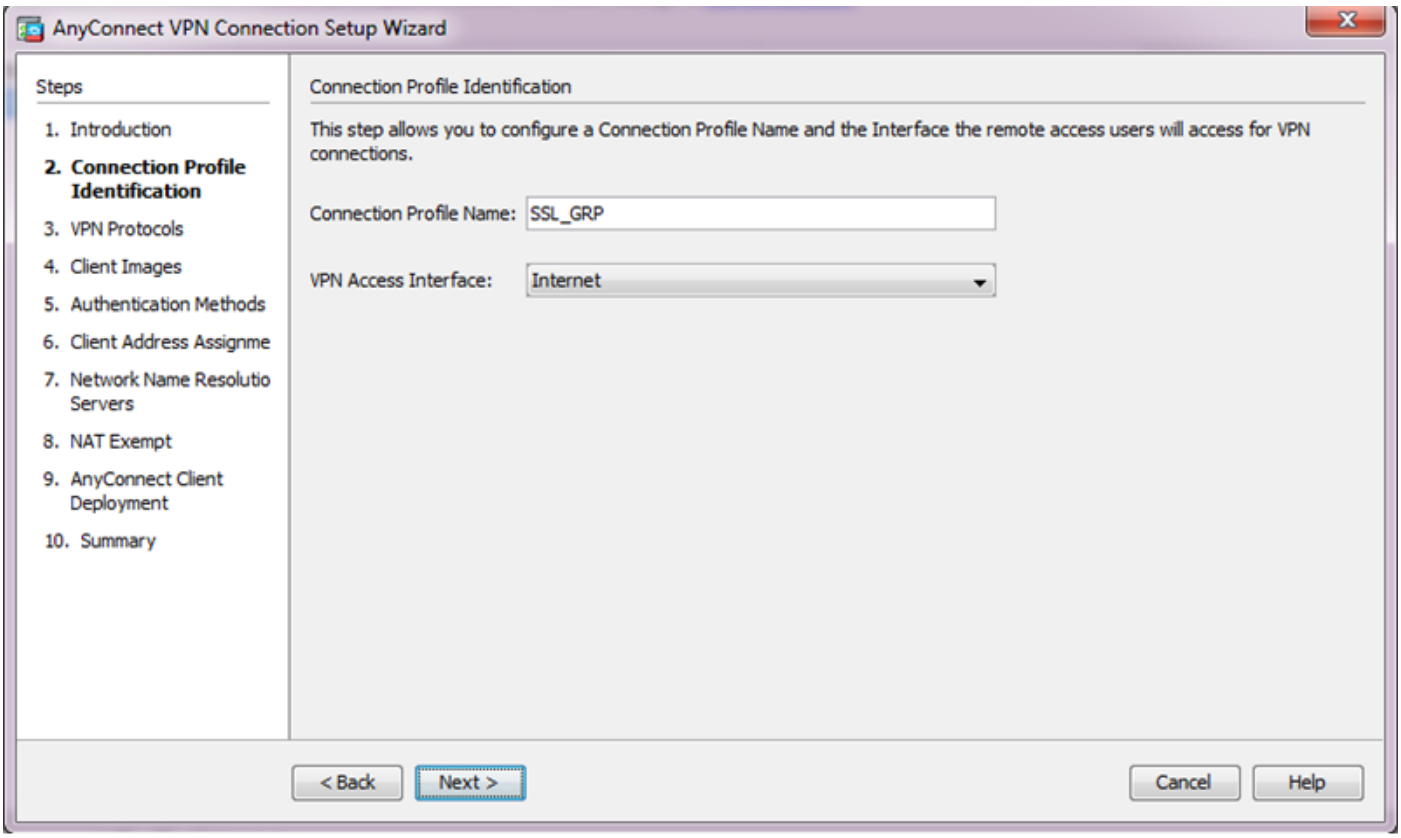
Sie können den AnyConnect Secure Mobility Client mit dem AnyConnect Configuration Wizard/CLI konfigurieren. Stellen Sie sicher, dass ein AnyConnect-Client-Paket in den Flash-Speicher oder auf die Festplatte der ASA-Firewall hochgeladen wurde, bevor Sie fortfahren.

Führen Sie die folgenden Schritte aus, um AnyConnect Secure Mobility Client über den Konfigurationsassistenten zu konfigurieren:

1. Melden Sie sich bei ASDM an, und navigieren Sie zu Wizards > VPN Wizards > AnyConnect VPN Wizard, um den Konfigurationsassistenten zu starten, und klicken Sie auf Next (Weiter).



2. Geben Sie den Namen des Verbindungsprofils ein, wählen Sie im Dropdown-Menü "VPN Access Interface" die Schnittstelle aus, an der das VPN terminiert werden soll, und klicken Sie auf Next (Weiter).



3. Aktivieren Sie das Kontrollkästchen SSL, um Secure Sockets Layer (SSL) zu aktivieren. Unter Device Certificate (Gerätezertifikat) können Sie ein von einer vertrauenswürdigen

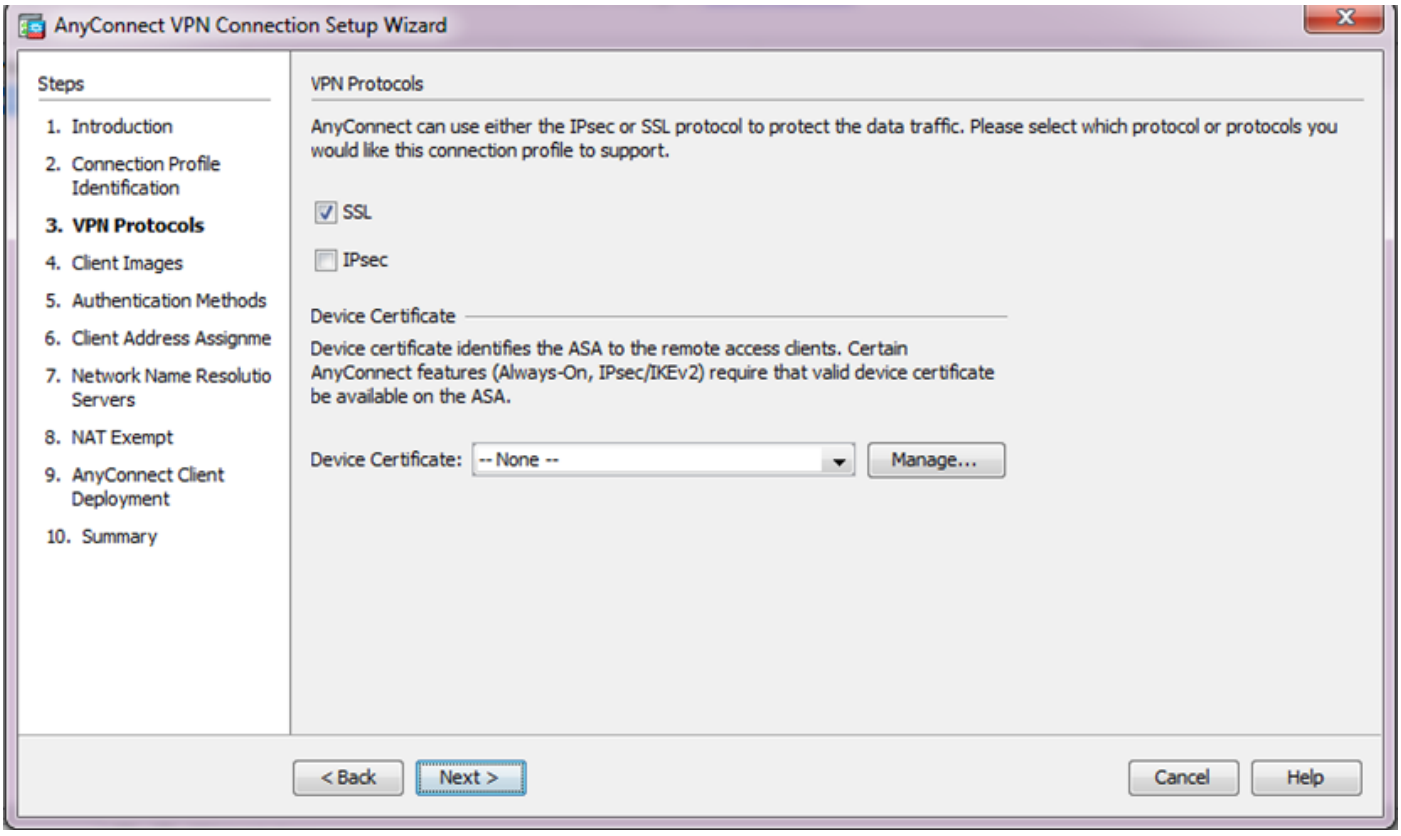
Zertifizierungsstelle (z. B. Verisign oder Entrust) ausgestelltes Zertifikat oder ein selbstsigniertes Zertifikat angeben. Wenn das Zertifikat bereits auf der ASA installiert ist, kann es über das Dropdown-Menü ausgewählt werden.

---

1. Hinweis: Dieses Zertifikat ist das serverseitige Zertifikat, das von ASA an SSL-Clients übermittelt wird. Wenn derzeit keine Serverzertifikate auf der ASA installiert sind, sondern nur ein selbstsigniertes Zertifikat generiert werden muss, klicken Sie auf Verwalten.

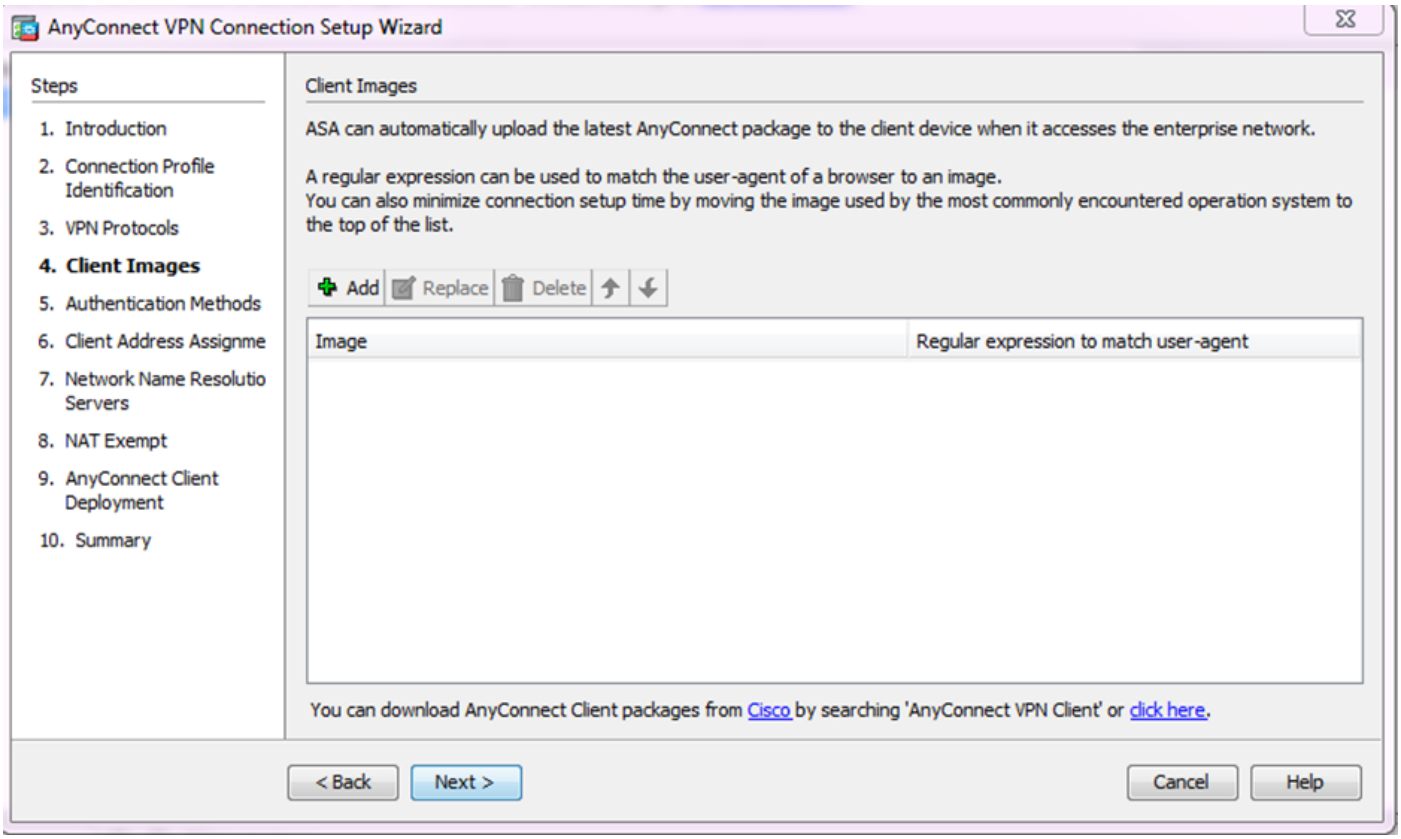
Um ein Drittanbieterzertifikat zu installieren, führen Sie die Schritte aus, die im Dokument ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example (ASA 8.x – manuelle Installation von Drittanbieterzertifikaten zur Verwendung mit dem WebVPN-Konfigurationsbeispiel) von Cisco beschrieben sind.

- Aktivieren Sie die VPN-Protokolle und das Gerätezertifikat.
- Klicken Sie auf Next (Weiter).

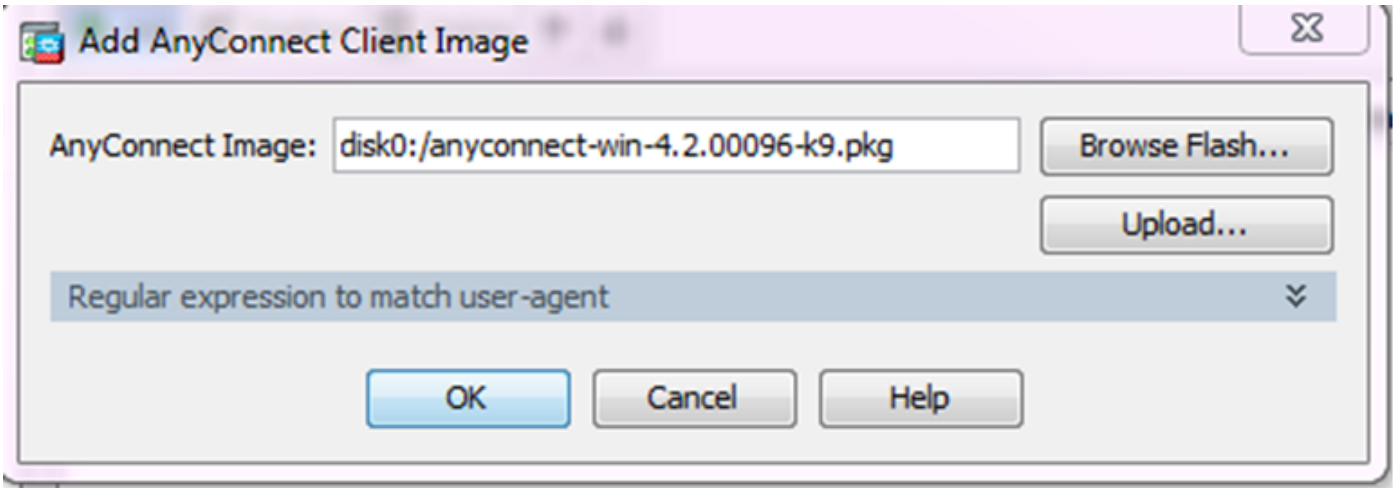


4. Klicken Sie auf Hinzufügen, um das AnyConnect-Client-Paket (.pkg-Datei) vom lokalen Laufwerk oder vom Flash-Speicher/Datenträger der ASA hinzuzufügen.

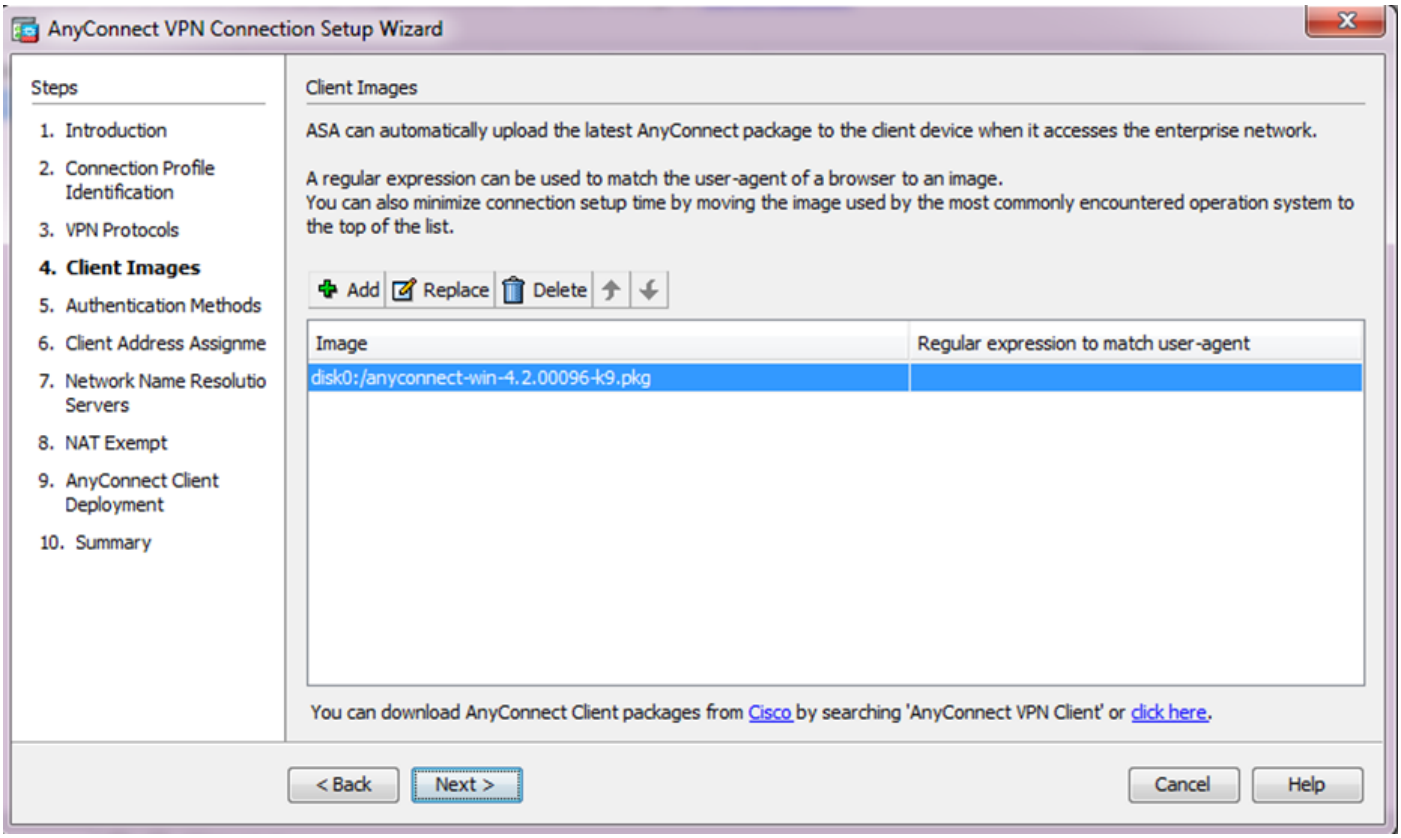
Klicken Sie auf Flash durchsuchen, um das Image vom Flash-Laufwerk hinzuzufügen, oder auf Hochladen, um das Image vom lokalen Laufwerk des Host-Computers hinzuzufügen.



- Sie können die Datei AnyConnect.pkg entweder von ASA Flash/Disk (wenn das Paket bereits vorhanden ist) oder vom lokalen Laufwerk hochladen.
- Flash durchsuchen: Wählen Sie das AnyConnect-Paket aus ASA Flash/Disk aus.
- Hochladen - Wählen Sie das AnyConnect-Paket aus dem lokalen Laufwerk des Host-Computers aus.
- Klicken Sie auf OK.

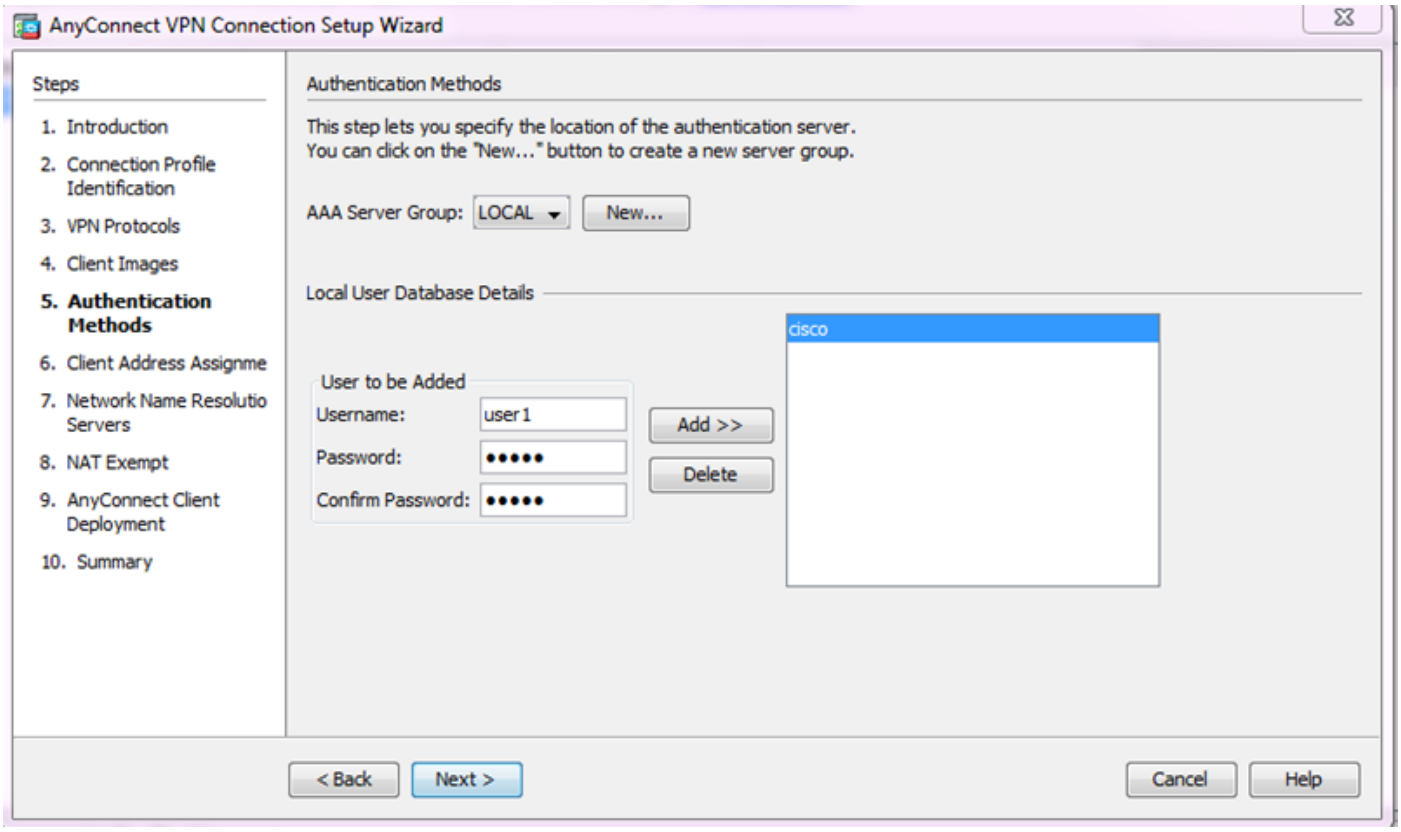


- Klicken Sie auf Next (Weiter).

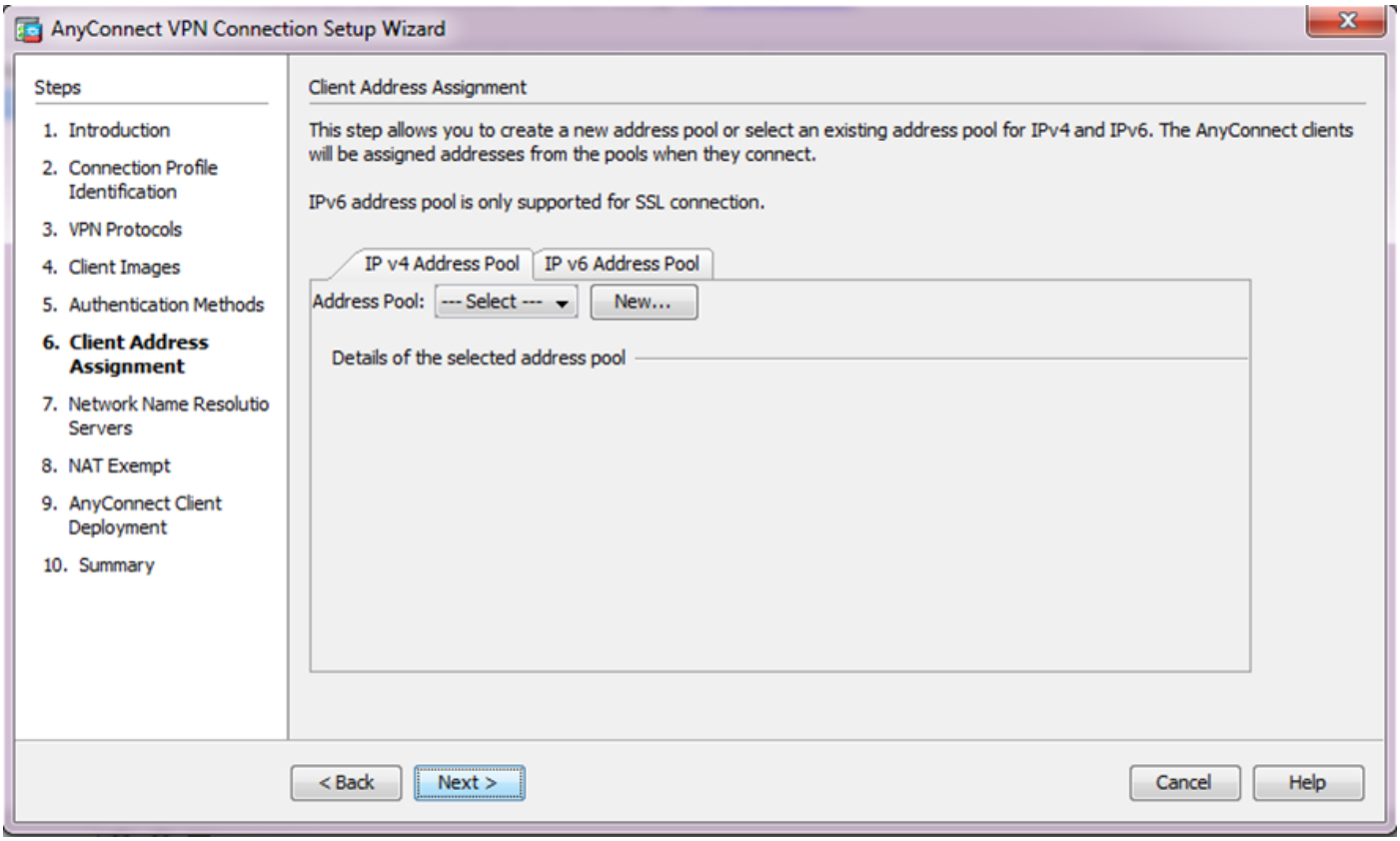


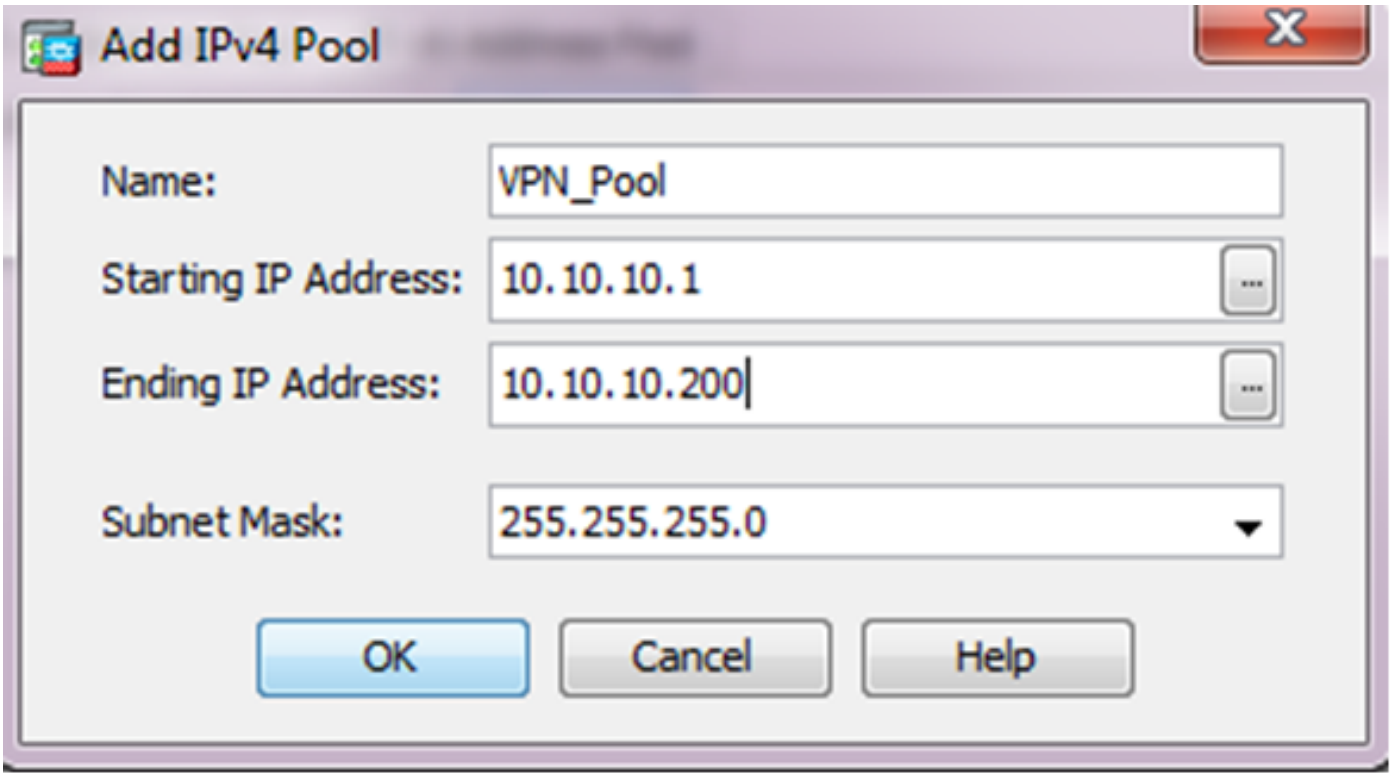
5. Die Benutzerauthentifizierung kann über die Servergruppen für Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA) abgeschlossen werden. Wenn die Benutzer bereits konfiguriert sind, wählen Sie LOKAL aus, und klicken Sie auf Weiter. Fügen Sie einen Benutzer zur lokalen Benutzerdatenbank hinzu, und klicken Sie auf Weiter.

Hinweis: In diesem Beispiel wird die LOKALE Authentifizierung konfiguriert, d. h. die lokale Benutzerdatenbank auf dem ASA wird für die Authentifizierung verwendet.

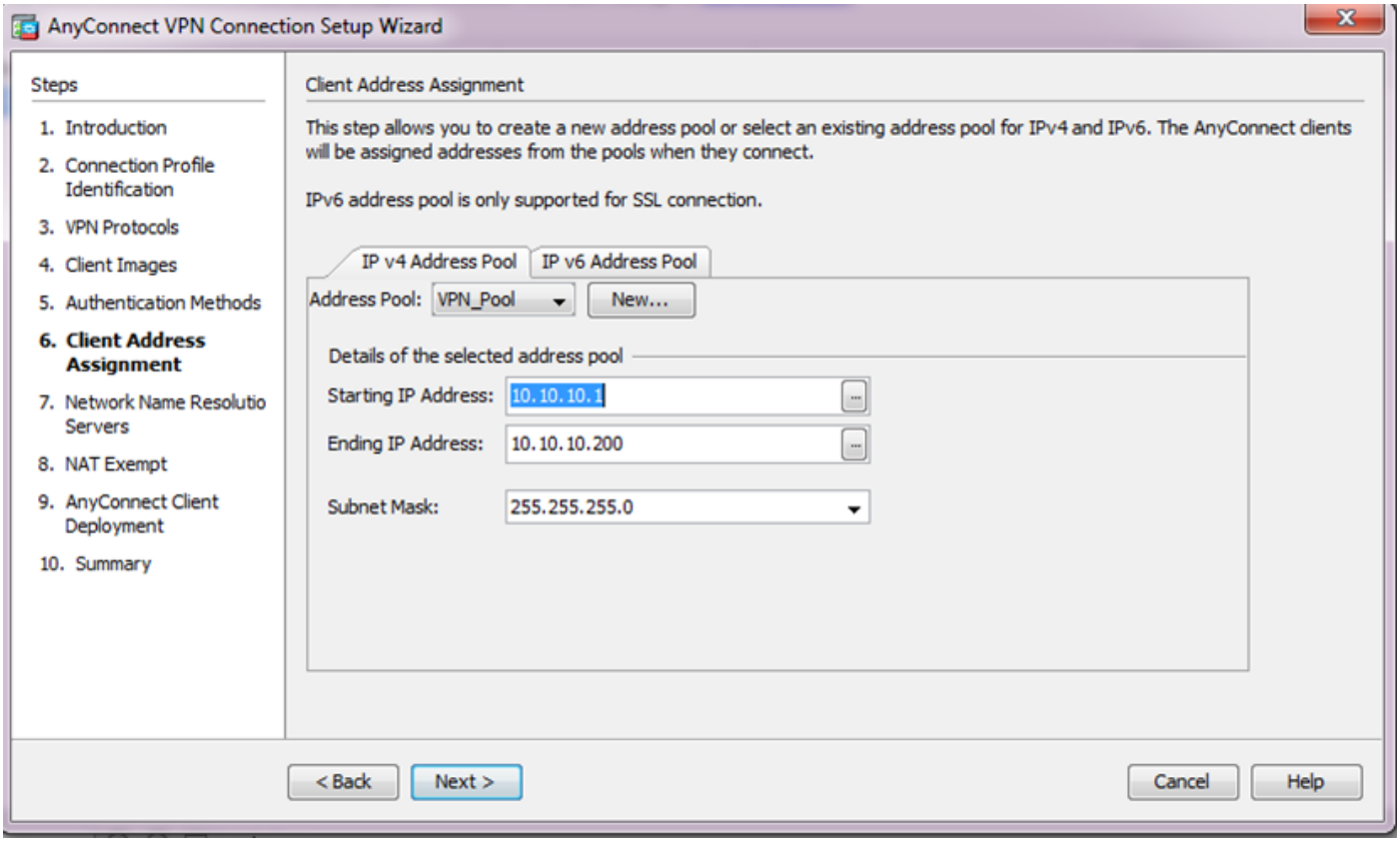


6. Stellen Sie sicher, dass der Adresspool für die VPN-Clients konfiguriert ist. Wenn bereits ein IP-Pool konfiguriert ist, wählen Sie ihn aus dem Dropdown-Menü aus. Falls nicht, klicken Sie zur Konfiguration auf Neu. Klicken Sie abschließend auf Weiter.

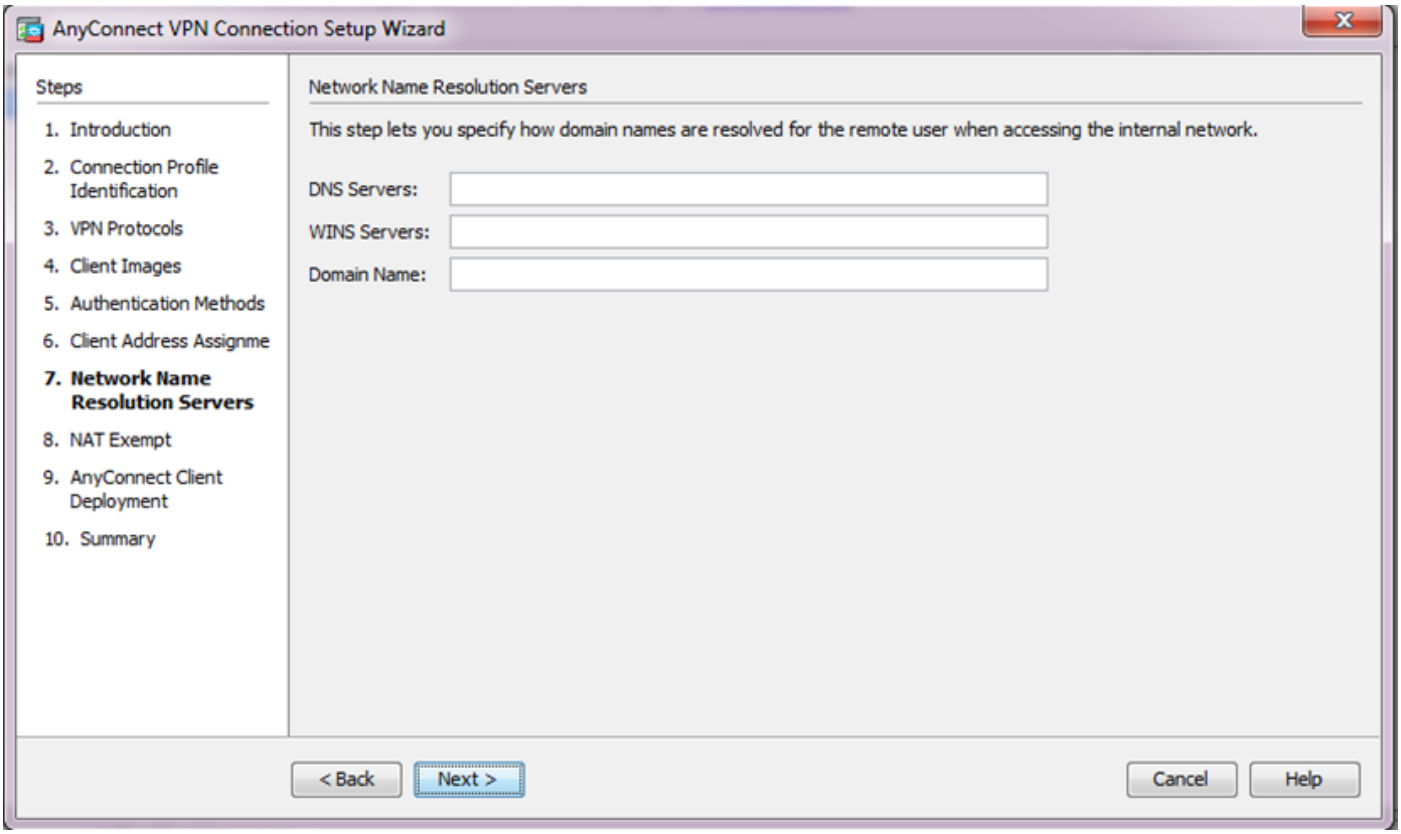




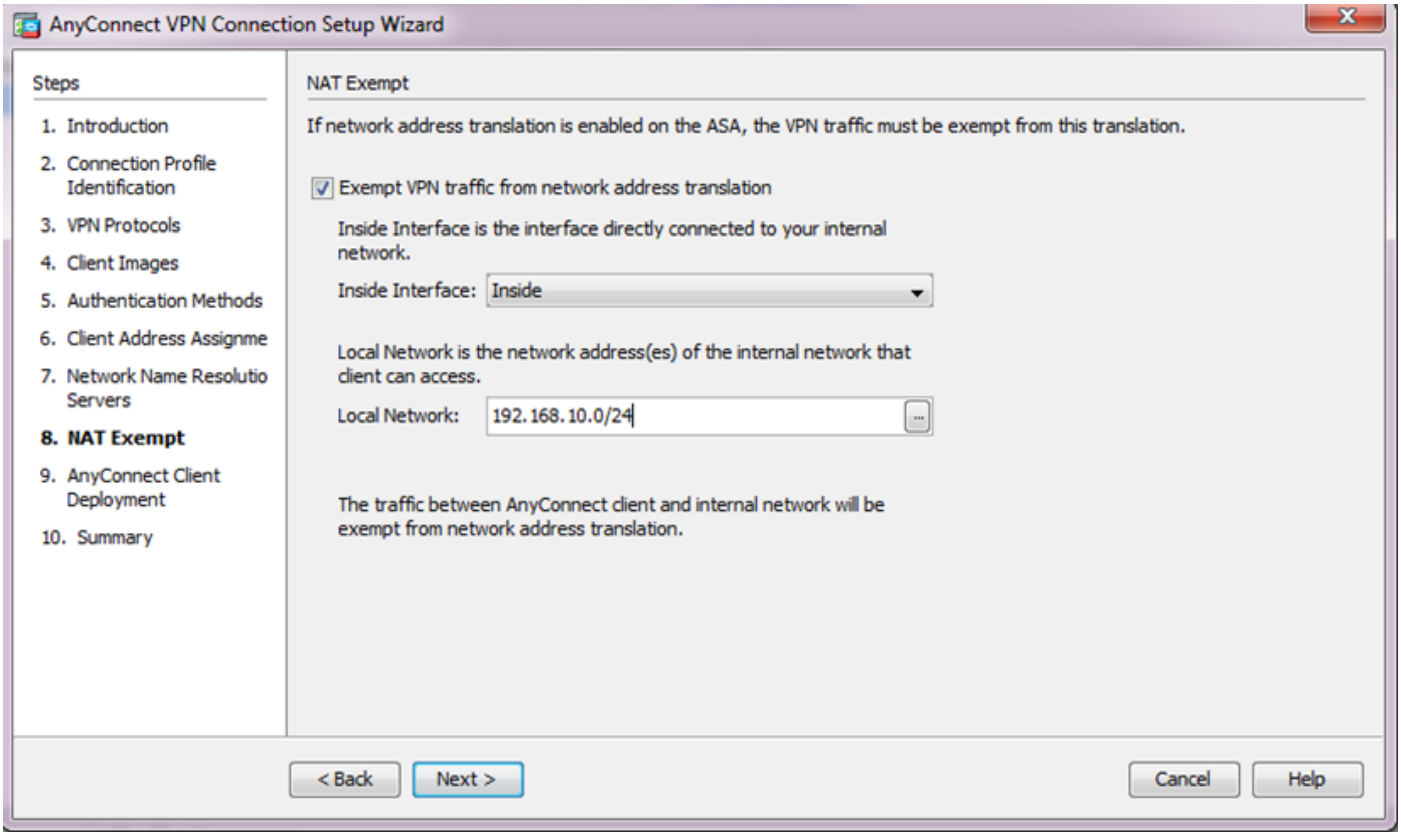
- Klicken Sie auf Next (Weiter).



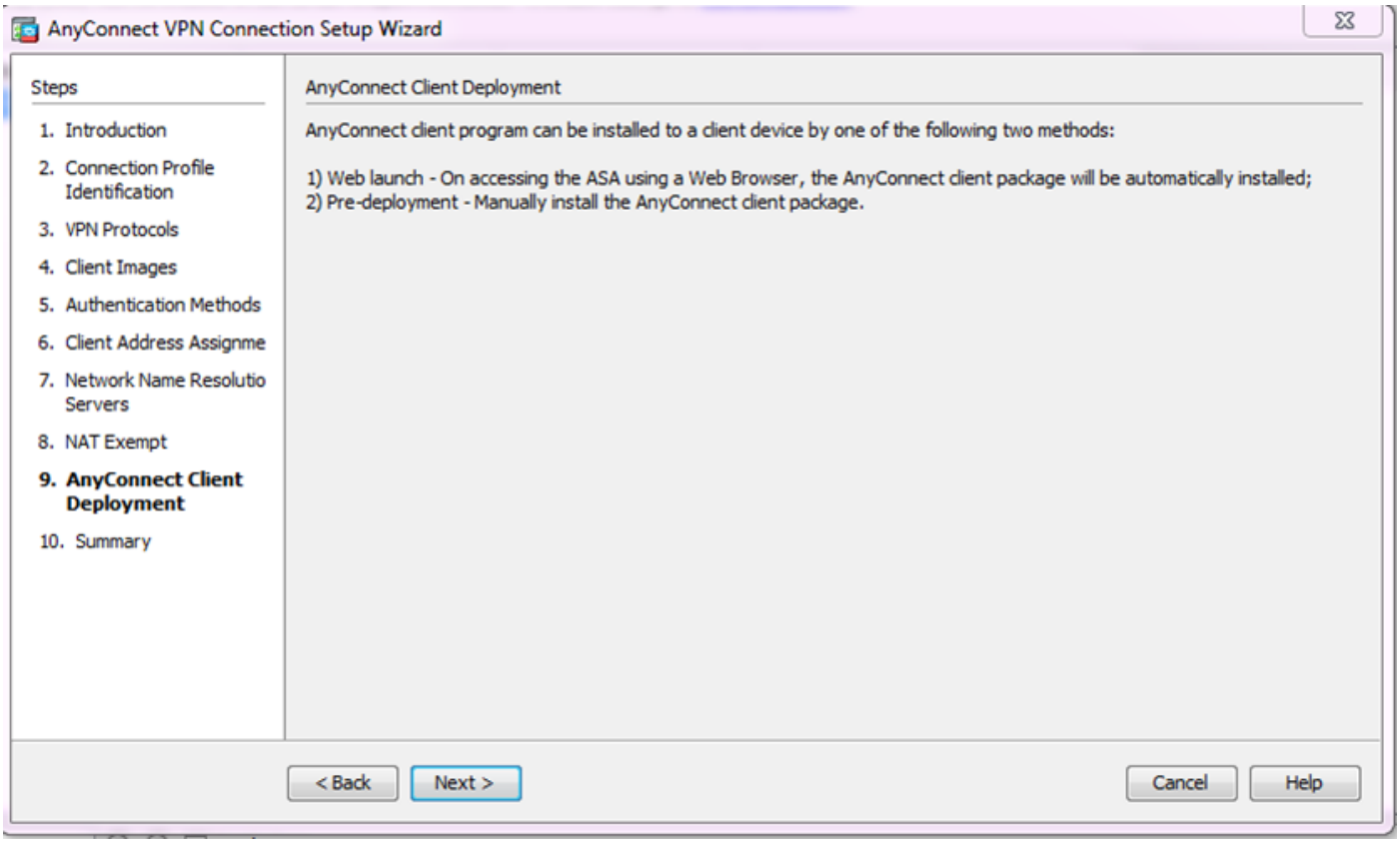
7. Konfigurieren Sie optional die DNS-Server (Domain Name System) und die DNSs in den Feldern DNS und Domänenname, und klicken Sie dann auf Weiter.



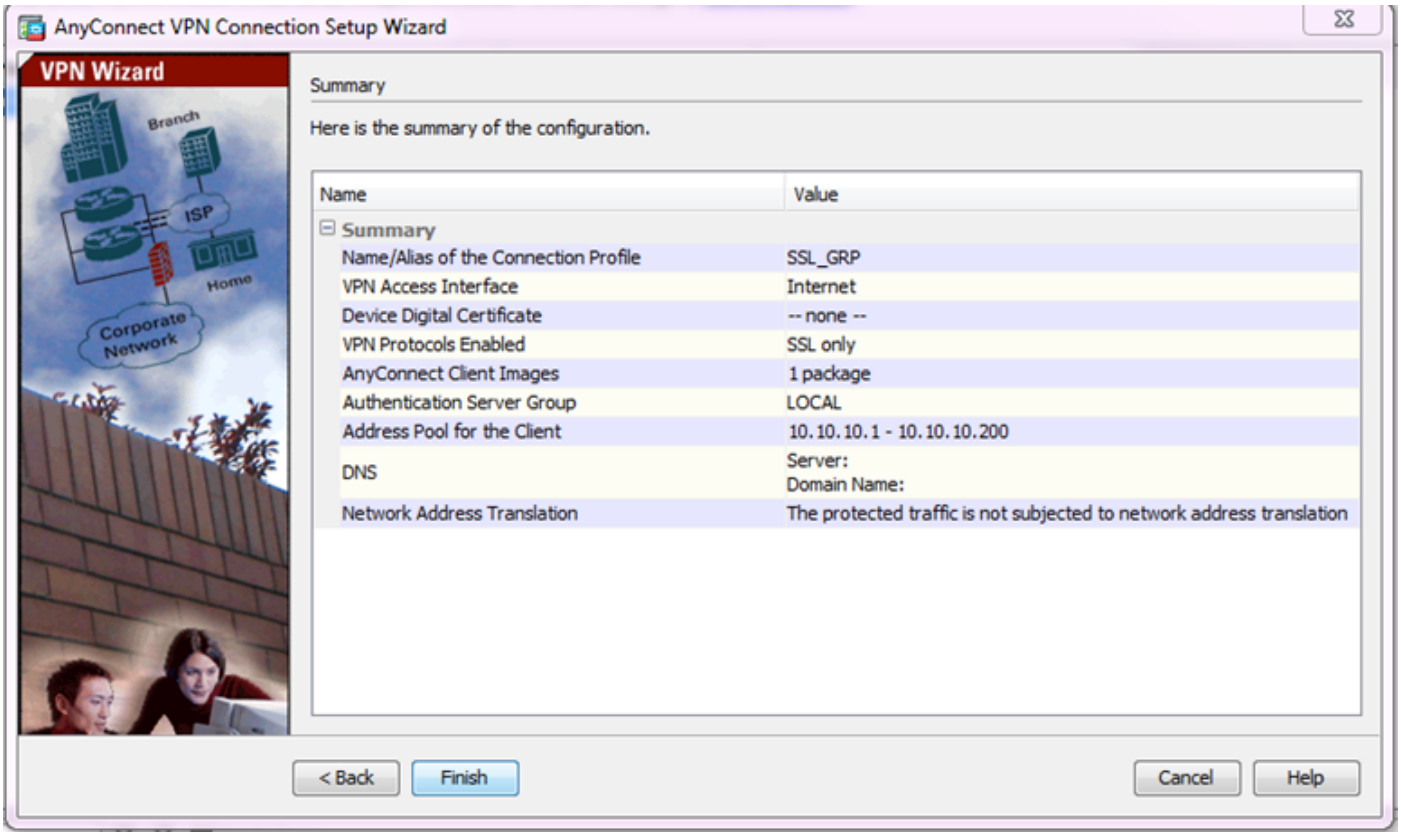
8. Stellen Sie sicher, dass der Datenverkehr zwischen dem Client und dem internen Subnetz von jeder dynamischen Network Address Translation (NAT) ausgenommen werden muss. Aktivieren Sie das Kontrollkästchen VPN-Datenverkehr von der Netzwerkadressenumwandlung ausnehmen, und konfigurieren Sie die LAN-Schnittstelle, die für die Ausnahme verwendet wird. Geben Sie außerdem das lokale Netzwerk an, das ausgenommen werden muss, und klicken Sie auf Weiter.



9. Klicken Sie auf Weiter.



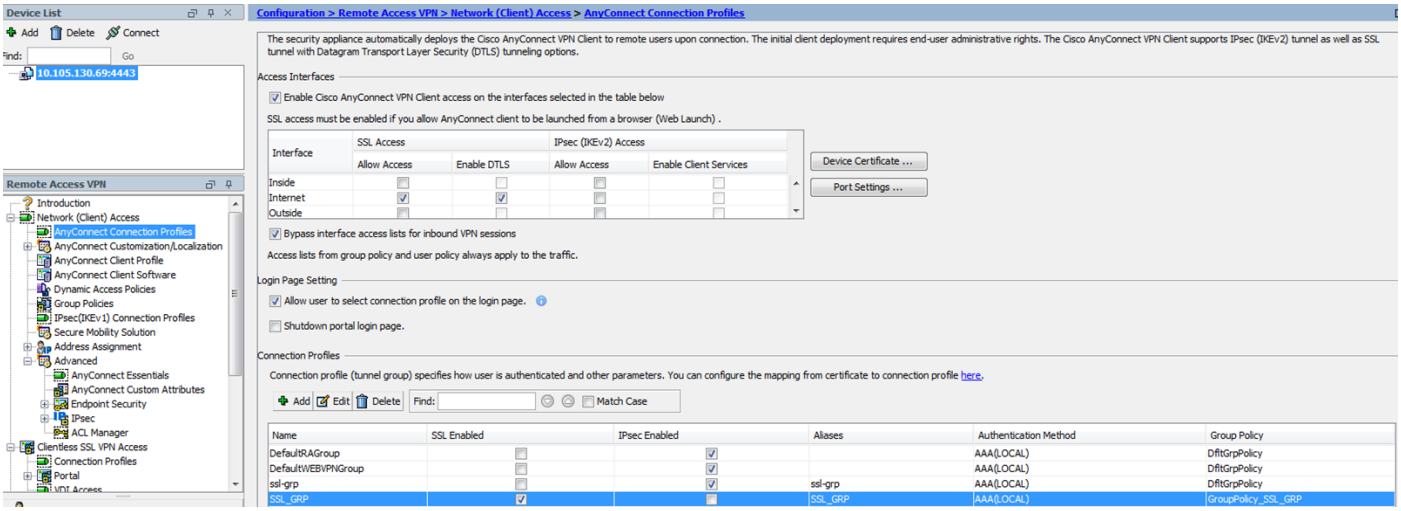
10. Im letzten Schritt wird die Zusammenfassung angezeigt. Klicken Sie auf Fertig stellen, um die Einrichtung abzuschließen.



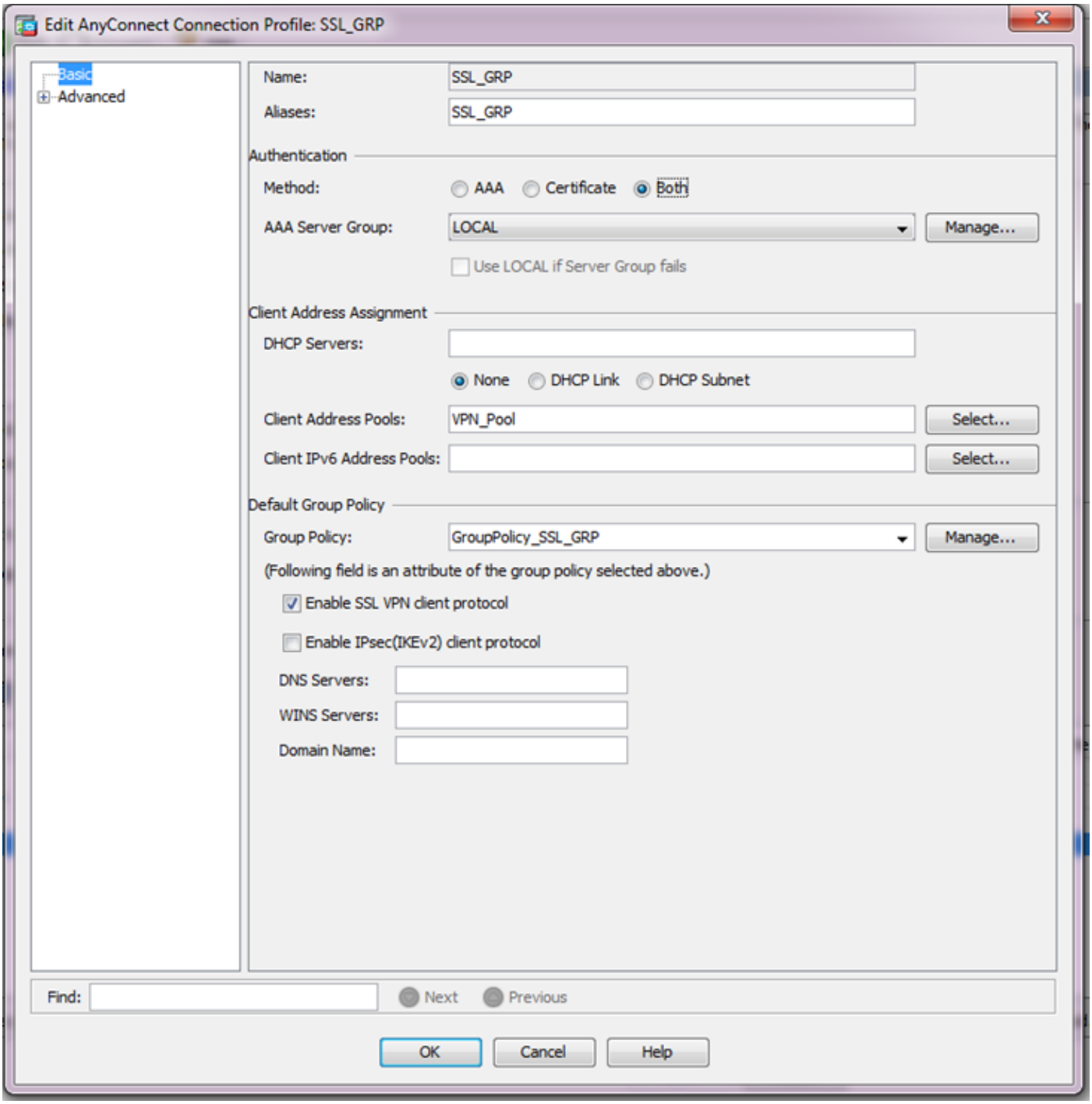
Die AnyConnect-Client-Konfiguration ist jetzt abgeschlossen. Wenn Sie AnyConnect jedoch über

den Konfigurationsassistenten konfigurieren, wird die Authentifizierungsmethode standardmäßig als AAA konfiguriert. Um die Clients über Zertifikate und Benutzername/Kennwort zu authentifizieren, muss die Tunnelgruppe (Verbindungsprofil) so konfiguriert werden, dass sie Zertifikate und AAA als Authentifizierungsmethode verwendet.

- Navigieren Sie zu Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles.
- Es sollte das neu hinzugefügte Verbindungsprofil SSL_GRP aufgeführt werden.



- Um AAA und Authentifizierung über Zertifikate zu konfigurieren, wählen Sie das Verbindungsprofil SSL_GRP aus, und klicken Sie auf Bearbeiten.
- Wählen Sie unter Authentication Method die Option Both aus.



Konfigurieren der CLI für 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
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Hinweis: Das Output-Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte show-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der show-Befehlsausgabe anzuzeigen.

Stellen Sie sicher, dass der CA-Server aktiviert ist.

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!!
```

Vergewissern Sie sich, dass der Benutzer nach dem Hinzufügen angemeldet sein kann:

<#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
```

Sie können die Details der AnyConnect-Verbindung entweder über die CLI oder ASDM überprüfen.

Über 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 :
```

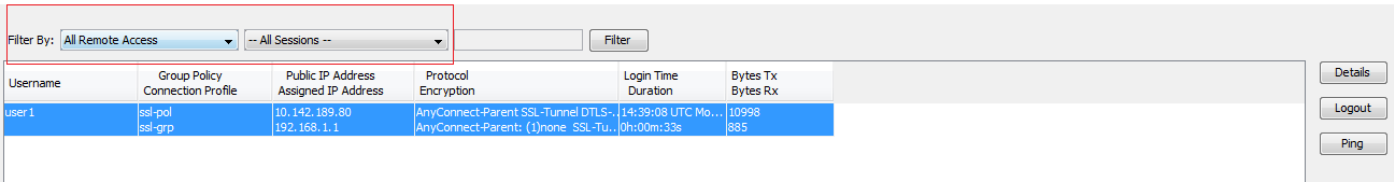
Über ASDM

- Navigieren Sie zu Monitoring > VPN > VPN Statistics > Sessions (Überwachung > VPN > VPN-Statistik > Sitzungen).
- Wählen Sie Filtern nach als allen Remote-Zugriff aus.
- Sie können eine der beiden Aktionen für den ausgewählten AnyConnect-Client ausführen.

Details - Weitere Informationen zur Sitzung

Abmelden: Manuelles Abmelden vom Headend

Ping: Pingen des AnyConnect-Clients vom Headend



Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

> Hinweis: Lesen Sie den Artikel Important Information on Debug Commands (Wichtige Informationen zu Debug-Befehlen), bevor Sie debug-Befehle verwenden.

> Vorsicht: Auf der ASA können Sie verschiedene Debug-Ebenen festlegen. Standardmäßig wird Ebene 1 verwendet. Wenn Sie die Debug-Ebene ändern, kann die Ausführlichkeit der Debugs zunehmen. Gehen Sie dabei besonders in Produktionsumgebungen vorsichtig vor.

- debuggen crypto ca
- debuggen crypto ca server
- Debuggen von Crypto CA-Nachrichten
- Verschlüsselungstransaktionen debuggen
- debuggen webvpn anyconnect

Diese Debug-Ausgabe zeigt an, wann der CA-Server mit dem Befehl no shutdown aktiviert wird.

<#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!
```

Diese Debug-Ausgabe zeigt die Registrierung des Clients

<#root>

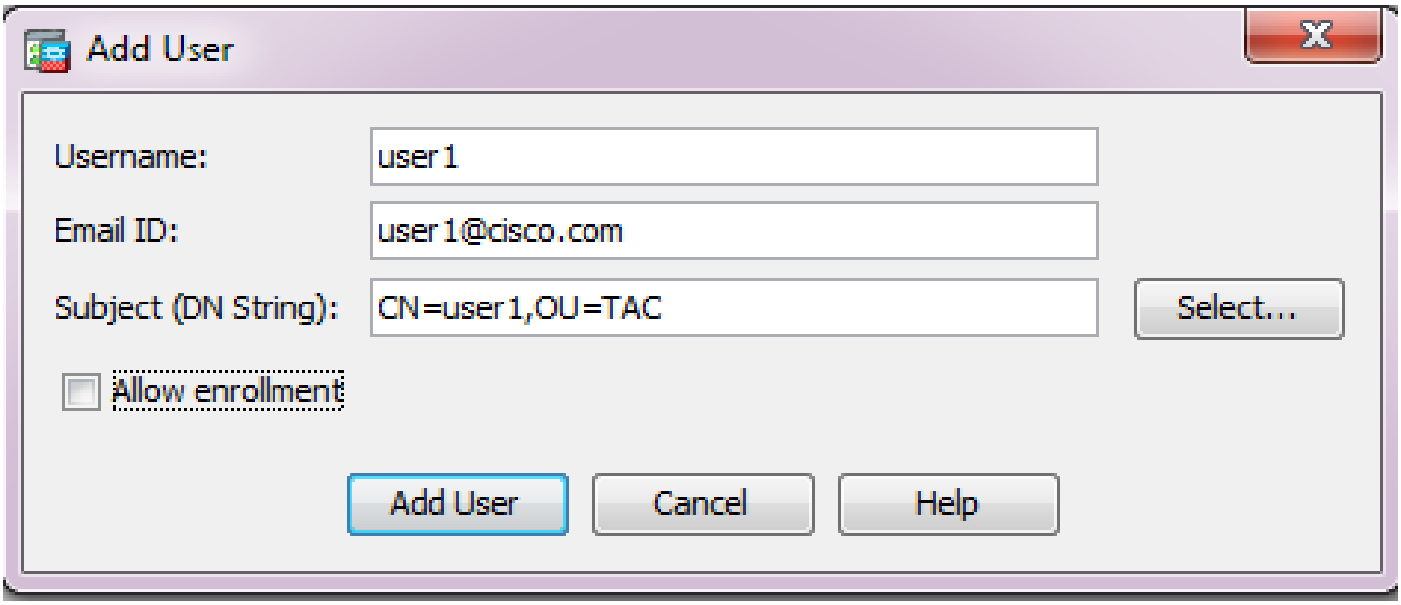
```
ASA# debug crypto ca 255
ASA# debug crypto ca server 255
ASA# debug crypto ca message 255
ASA# debug crypto ca transaction 255
```

```
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
```

Die Registrierung des Kunden kann unter folgenden Bedingungen fehlschlagen:

Szenario 1.

- Der Benutzer wird ohne Berechtigung zur Registrierung in der Datenbank des Zertifizierungsstellen-Servers erstellt.



CLI-Äquivalent:

<#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
```

- Wenn der Benutzer sich nicht registrieren darf und versucht, das OTP für den Benutzer zu generieren/per E-Mail zu versenden, wird diese Fehlermeldung generiert.

Szenario 2.

- Überprüfen Sie mit dem Befehl show run webvpn den Port und die Schnittstelle, auf der das Registrierungsportal verfügbar ist. Der Standard-Port ist 443, kann jedoch geändert werden.

- Stellen Sie sicher, dass der Client über die Netzwerkerreichbarkeit zur IP-Adresse der Schnittstelle verfügt, auf der WebVPN auf dem Port aktiviert ist, der für den erfolgreichen Zugriff auf das Registrierungsportal verwendet wird.

In folgenden Fällen kann der Client möglicherweise nicht auf das Registrierungsportal der ASA zugreifen:

1. Wenn ein zwischengeschaltetes Gerät die eingehenden Verbindungen vom Client zur WebVPN-IP der ASA auf dem angegebenen Port blockiert.
2. Der Status der Schnittstelle ist ausgefallen, auf der webvpn aktiviert ist.

- Diese Ausgabe zeigt, dass das Registrierungsportal unter der IP-Adresse der Schnittstelle Internet auf dem benutzerdefinierten Port 4433 verfügbar ist.

<#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
```

Szenario 3.

- Der Standardspeicherort des CA Server-Datenbankspeichers ist der Flash-Speicher der ASA.
- Stellen Sie sicher, dass der Flash-Speicher über freien Speicherplatz zum Generieren und Speichern der pkcs12-Datei für den Benutzer während der Registrierung verfügt.
- Falls der Flash-Speicher nicht über genügend freien Speicherplatz verfügt, kann ASA den Registrierungsprozess des Clients nicht abschließen und generiert die folgenden Debug-Protokolle:

<#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
```

Zugehörige Informationen

- Cisco Adaptive Security Appliances der Serie ASA 5500
- Fehlerbehebungsleitfaden für AnyConnect VPN-Client – häufige Probleme
- Management, Überwachung und Fehlerbehebung von AnyConnect-Sitzungen
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.