

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[ASA as a Local CA Server](#)

[Step 1. Configure and enable the Local CA Server on ASA](#)

[Step 2. Create and add users to the ASA database](#)

[Step 3. Enable webvpn on the WAN interface](#)

[Step 4. Import the certificate on the client machine](#)

[ASA as a SSL gateway for AnyConnect Clients](#)

[ASDM AnyConnect Configuration Wizard](#)

[Configure CLI for AnyConnect](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to setup a Cisco Adaptive Security Appliance (ASA) as a Certificate Authority (CA) server and as a Secure Sockets Layer (SSL) gateway for Cisco AnyConnect Secure Mobility Clients.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic ASA configuration that runs software version 9.1.x
- ASDM 7.3 or higher

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series ASA that runs software version 9.1(6)
- AnyConnect Secure Mobility Client version 4.x for Windows
- PC which runs an supported OS per the [Compatibility Chart](#).
- Cisco Adaptive Security Device Manager (ASDM) version 7.3

Note: Download the AnyConnect VPN Client package (anyconnect-win*.pkg) from the Cisco [Software Download](#) ([registered](#) customers only) . Copy the AnyConnect VPN client to the ASA's flash memory, which is to be downloaded to the remote user computers in order to establish the SSL VPN connection with the ASA. Refer to the [Installing the AnyConnect Client](#) section of the ASA configuration guide for more information.

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

Background Information

The Certificate authority on the ASA provides these functionalities:

- Integrates basic certificate authority operation on the ASA.
- Deploys certificates.
- Provides secure revocation checking of issued certificates.
- Provides a certificate authority on the ASA for use with browser-based(WebVPN) and client-based(AnyConnect) SSL VPN connections.
- Provides trusted digital certificates to users, without the need to rely on external certificate authorization.
- Provides a secure, in-house authority for certificate authentication and offers straightforward user enrollment by means of a website login.

Guidelines and Limitations

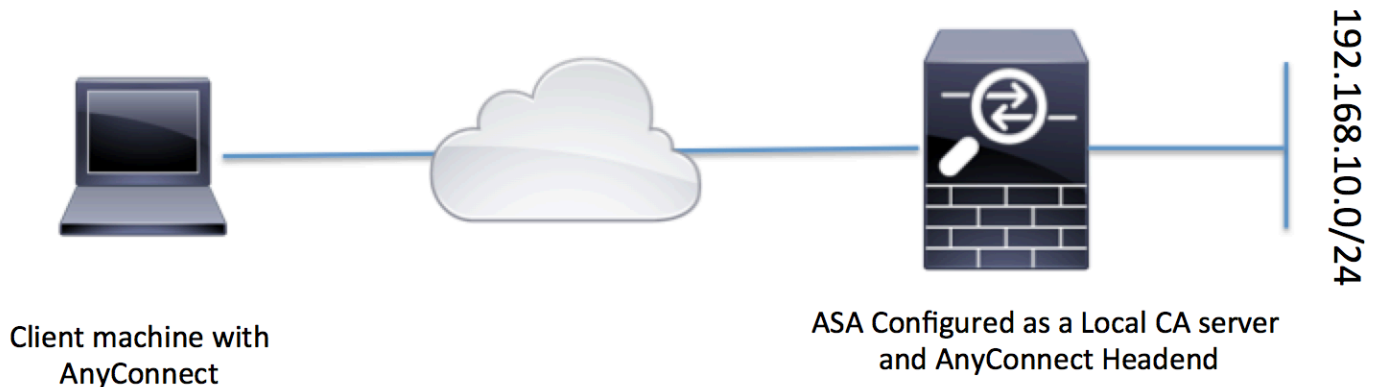
- Supported in routed and transparent firewall mode.
- Only one local CA server at a time can be resident on an ASA.
- ASA as a Local CA server feature is not supported in a failover setup.
- The ASA as of now acting as a Local CA server only supports generation of SHA1 certificates.
- Local CA server can be used for browser-based and client-based SSL VPN connections. Currently not supported for IPsec.
- Does not support VPN load balancing for the local CA.
- The local CA cannot be a subordinate to another CA. It can act only as the root CA.
- Currently the ASA cannot enroll to the local CA server for the identity certificate.
- When a certificate enrollment is completed, the ASA stores a PKCS12 file containing the user's keypair and certificate chain, which requires about 2 KB of flash memory or disk space per enrollment. The actual amount of disk space depends on the configured RSA key size and certificate fields. Keep this guideline in mind when adding a large number of pending certificate enrollments on an ASA with a limited amount of available flash memory, because these PKCS12 files are stored in flash memory for the duration of the configured enrollment retrieval timeout.

Configure

This section describes how to configure the Cisco ASA as a Local CA server.

Note: Use the [Command Lookup Tool](#) (registered customers only) in order to obtain more information on the commands used in this section.

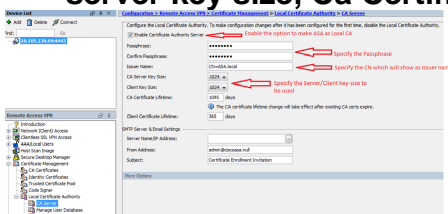
Network Diagram



ASA as a Local CA Server

Step 1. Configure and enable the Local CA Server on ASA

- Navigate to **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**. Check the **Enable Certificate Authority server** option.
- Configure Passphrase. The Passphrase should be a minimum, 7 characters which is used to encode and save a PKCS12 file that includes the local CA certificate and key pair. The passphrase unlocks the PKCS12 archive if the CA certificate or keypair is lost.
- Configure the Issuer Name. This field would appear as Root Certificate CN. This can be specified in the following format: CN (Common Name), OU (Organisation unit), (O) Organisation , L (Locality) , S (State) and C (Country).
- **Optional Configuration:** Configure the SMTP Server and Email Server settings to ensure the OTP could be received to end clients via mail to complete the enrollment. You may configure hostname or IP address of your local Email/SMTP server. You may also configure **From address** and **Subject** field of the email which the clients would receive. By default, the From Address is **admin@<ASA hostname>.null** and the Subject is **Certificate Enrollment Invitation**.
- **Optional Configuration:** You may configure the optional parameters like **Client key size**, **CA server key size**, **Ca Certificate Lifetime** and **Client certificate lifetime** as well.



CLI equivalent:

These are additional fields that could be configured under Local CA Server configuration.

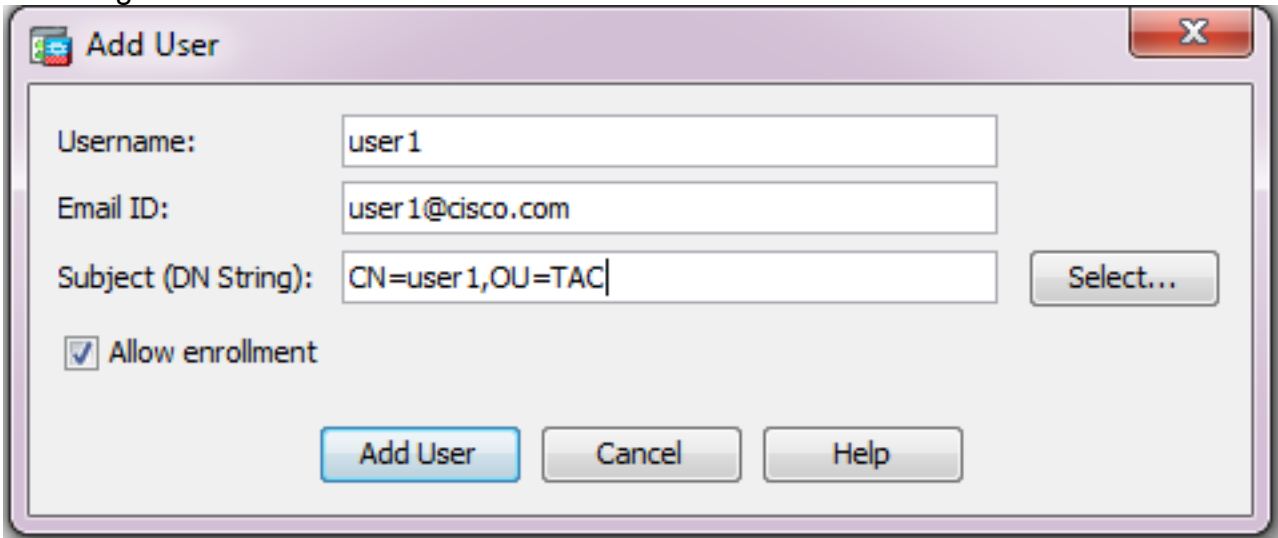
CRL	This is the CRL location on the ASA.
Distribution point URL	The default location is http://hostname.domain/+CSCOCA+/asa_ca.crl but the url could be modified.
Publish-CRL Interface and Port	To make the CRL available for HTTP download on a given interface and port, choose a publish-CRL interface from the drop-down list. Then enter the port number, which can be any port number from 1-65535. The default port number is TCP port 80.
CRL Lifetime	The Local CA updates and reissues the CRL every time a user certificate is revoked or unrevoked, but if there are no revocation changes, the CRL is reissued automatically once every CRL lifetime, the period of time you specify with the lifetime crl command during Local CA configuration. If you do not specify a CRL lifetime, the default time period is six hours .
Database Storage Location	<p>The ASA accesses and implements user information, issued certificates, and revocation lists using a local CA database. This database resides in local flash memory by default, or can be configured to reside on an external file system that is mounted and accessible to the ASA.</p> <p>Enter a default subject (DN string) to append to a username on issued certificates. The permitted DN attributes are provided in this list:</p> <ul style="list-style-type: none">• CN (Common Name)SN (Surname)• O (Organization Name)• L (Locality)• C (Country)• OU (Organization Unit)• EA (E-mail Address)• ST (State/Province)• T (Title)
Default Subject Name	
Enrollment Period	<p>Sets the enrollment time limit in hours within which user could retrieve the PKCS12 file from ASA.</p> <p>The default value is 24 hours.</p> <p>Note: If the enrollment period expires before the user retrieves the PKCS12 file that includes the user certificate, enrollment is not permitted.</p>
One Time Password Expiration	Defines the amount of time in hours that the OTP is valid for user enrollment. This time period begins when the user is allowed to enroll. The default value is 72 hours.
Certificate Expiration	Specifies the number of days before certificate expires that an initial reminder to reenroll is sent to certificate owners.
Reminder	

Step 2. Create and add users to the ASA database

- Navigate to **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database**. Click **Add**.



- Specify the user details viz. Username, Email ID and the subject name, as shown in this image.



The 'Add User' dialog box contains the following fields and controls:

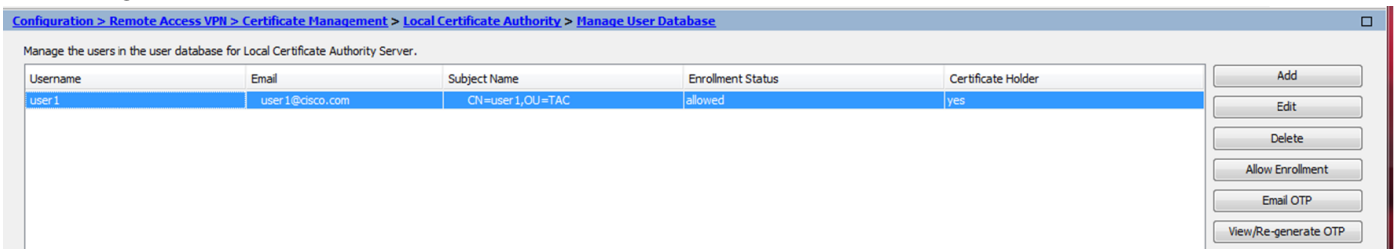
- Username:** user1
- Email ID:** user1@cisco.com
- Subject (DN String):** CN=user1,OU=TAC
- Select...** button
- ☒ **Allow enrollment**
- Add User** button
- Cancel** button
- Help** button

- Ensure that **Allow Enrollment** is checked so that you are allowed to enroll for the certificate.
- Click **Add User** to complete the user configuration.

CLI equivalent:

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

- After the user is added to the User Database, the enrollment status is shown as **Allowed to Enroll**.



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

Username	Email	Subject Name	Enrollment Status	Certificate Holder
user1	user1@cisco.com	CN=user1,OU=TAC	allowed	yes

Buttons: Add, Edit, Delete, Allow Enrollment, Email OTP, View/Re-generate OTP

CLI to verify the user status:

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

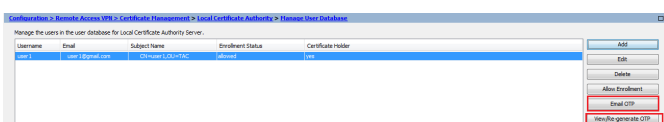
```
username: user1
email:    user1@cisco.com
dn:       CN=user1,OU=TAC
allowed:  19:03:11 UTC Thu Jan 14 2016
notified: 1 times
enrollment status: Allowed to Enroll
```

- After the user has been added to the User Database, the One Time Password (OTP), for the user to complete the enrollment, can be provided using either this:

Email the OTP (Requires SMTP server and Email Settings to be configured under the CA server configuration).

OR

Directly view the OTP and share with the user by clicking on View/Re-generate OTP. This can also be used to regenerate the OTP.



Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > Manage User Database

Manage the users in the user database for Local Certificate Authority Server.

Username	Email	Subject Name	Enrollment Status	Certificate Holder
user1	user1@cisco.com	CN=user1,OU=TAC	allowed	yes

Buttons: Add, Edit, Delete, Allow Enrollment, Email OTP, View/Re-generate OTP

CLI equivalent:

```
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
```

Step 3. Enable webvpn on the WAN interface

- Enable Web Access on the ASA for clients to request for 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
```

Step 4. Import the certificate on the client machine

- On the client workstation open a browser and navigate to the link in order to complete the enrollment.
- The **IP/FQDN** used in this link should be the IP of the interface on which **webvpn** is enabled in that step, which is **interface Internet**.

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

- Enter the username (configured on the ASA under Step 2 , option A) and the **OTP**, which was provided via **Email** or **manually**.

ASA - Local Certificate Authority

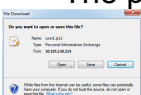
Username:

One-time Password:

NOTE: On successful authentication:

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

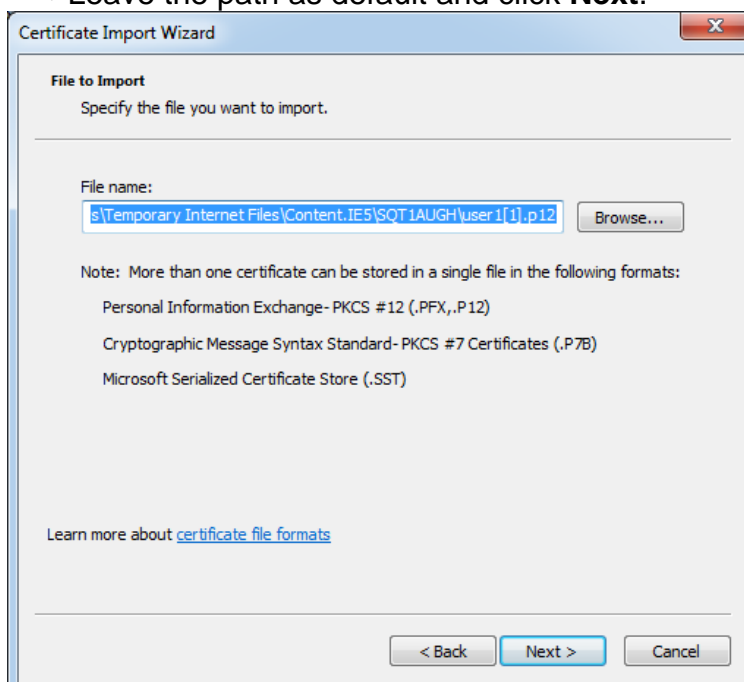
- Click **Open** to directly install the client certificate received from the ASA.
- The passphrase to install the client certificate is same as the OTP received earlier.



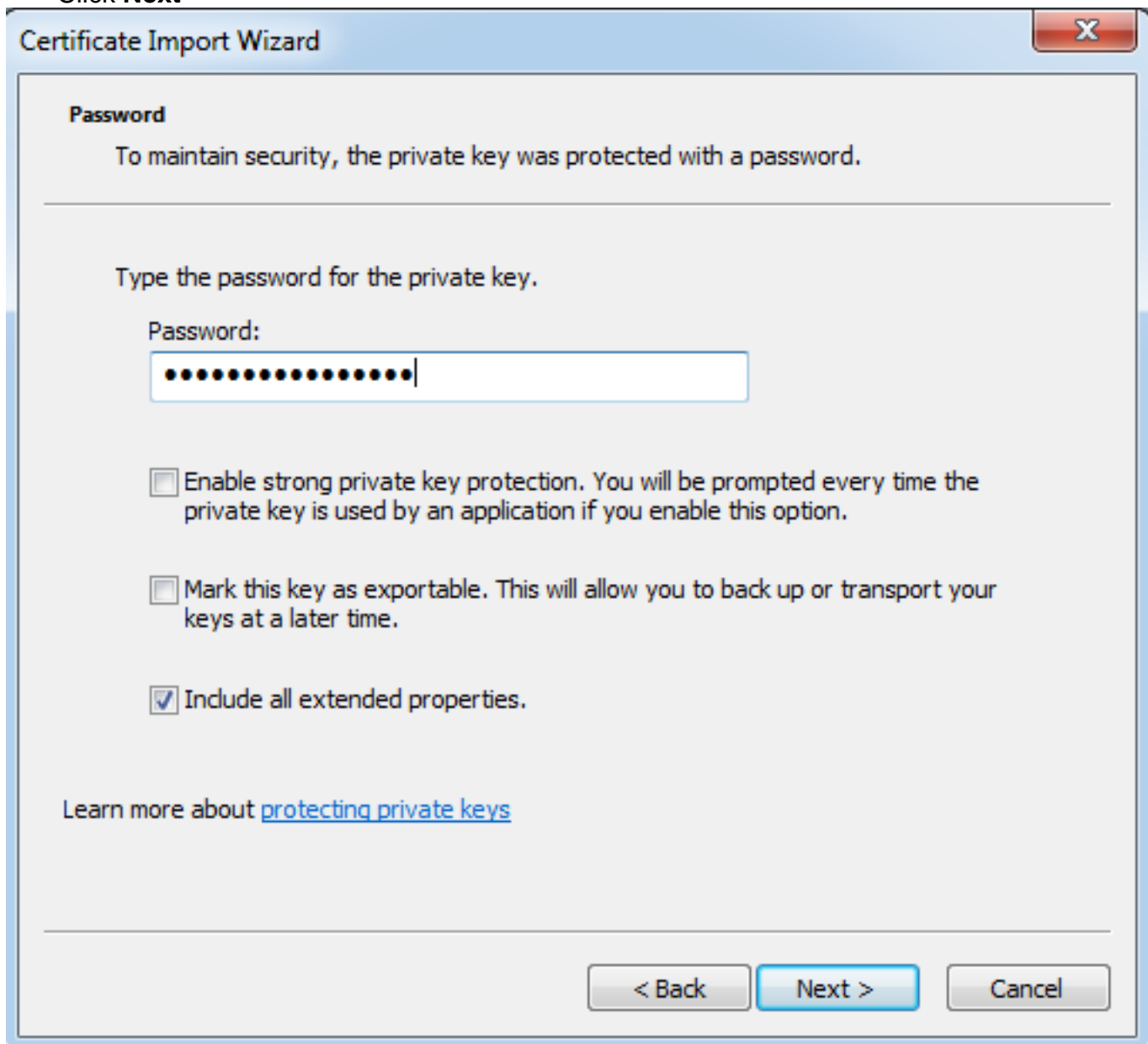
- Click **Next**.



- Leave the path as default and click **Next**.



- Enter the OTP in the Password field.
- You can select the option to **Mark this key as exportable** so that the key could be exported from the workstation in future if required.
- Click **Next**



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

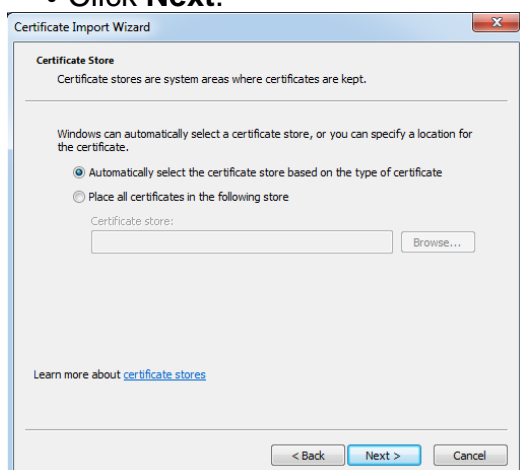
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Learn more about [protecting private keys](#)

< Back Next > Cancel

- You can manually install the certificate in a particular certificate store or leave it to automatically choose the store.
- Click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☒ Automatically select the certificate store based on the type of certificate

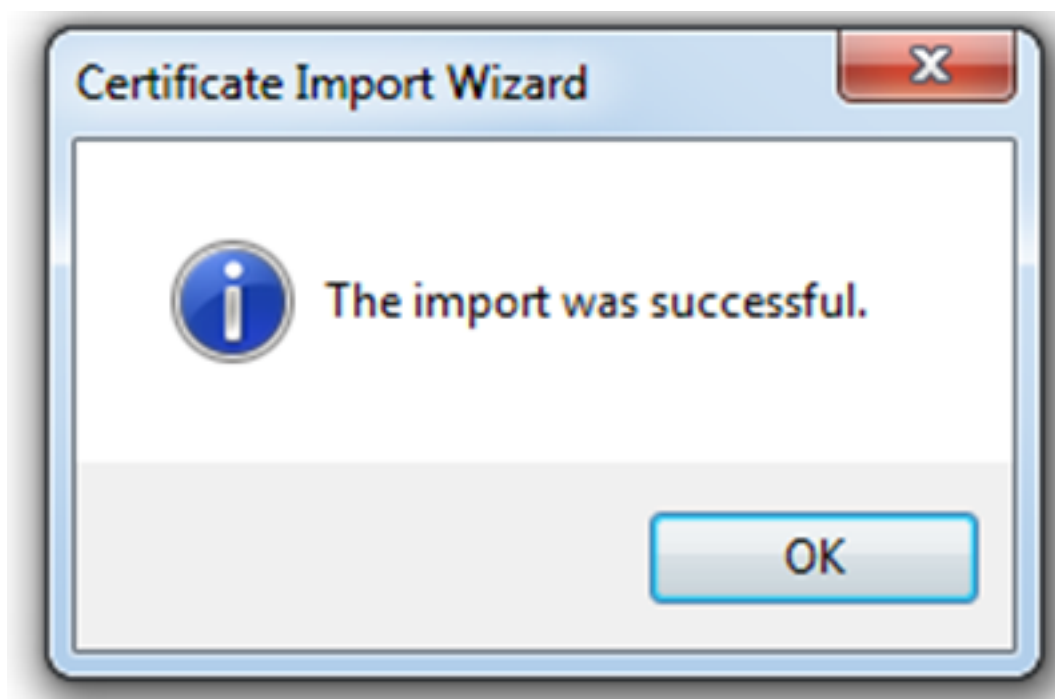
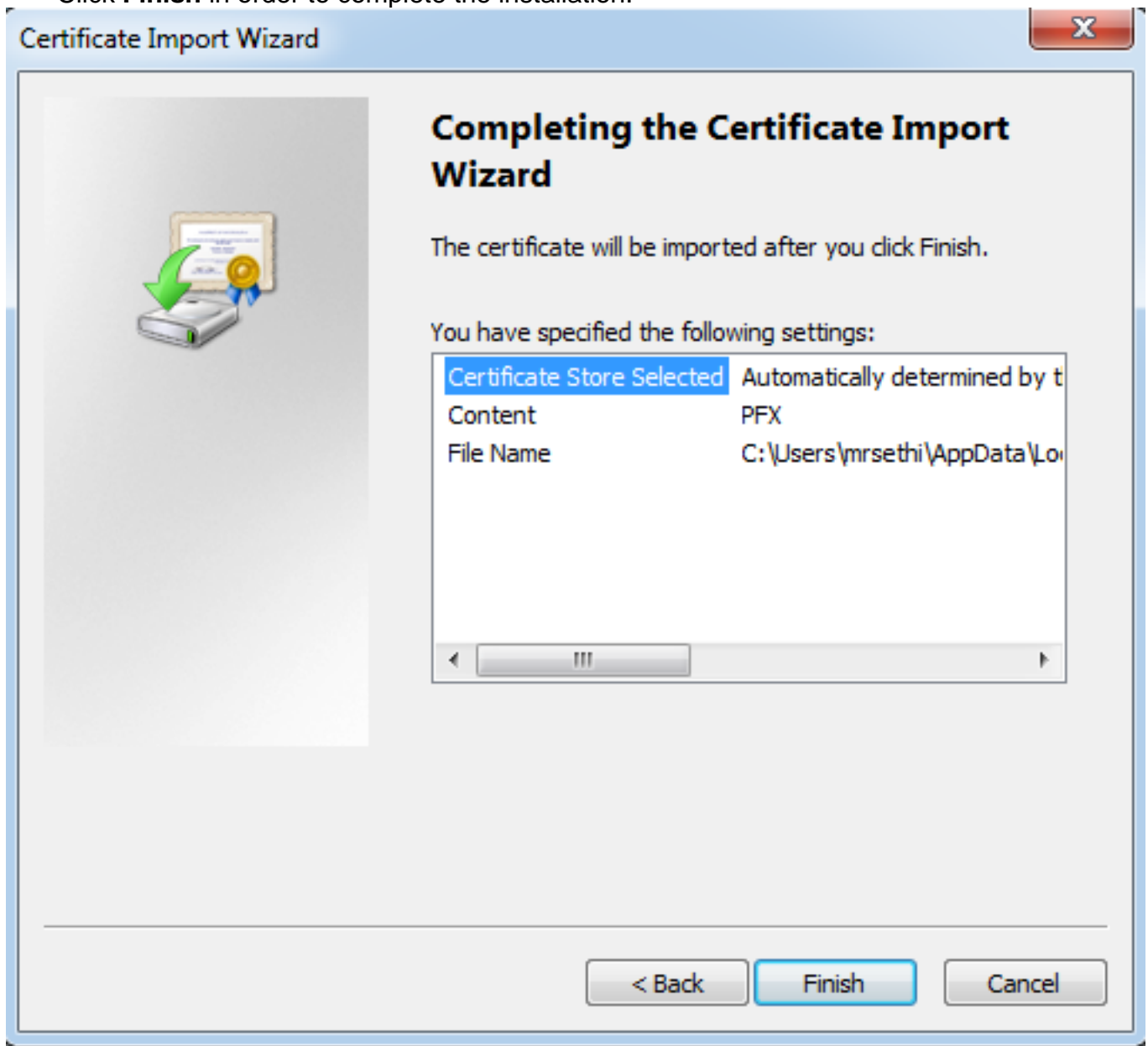
☐ Place all certificates in the following store

Certificate store: Browse...

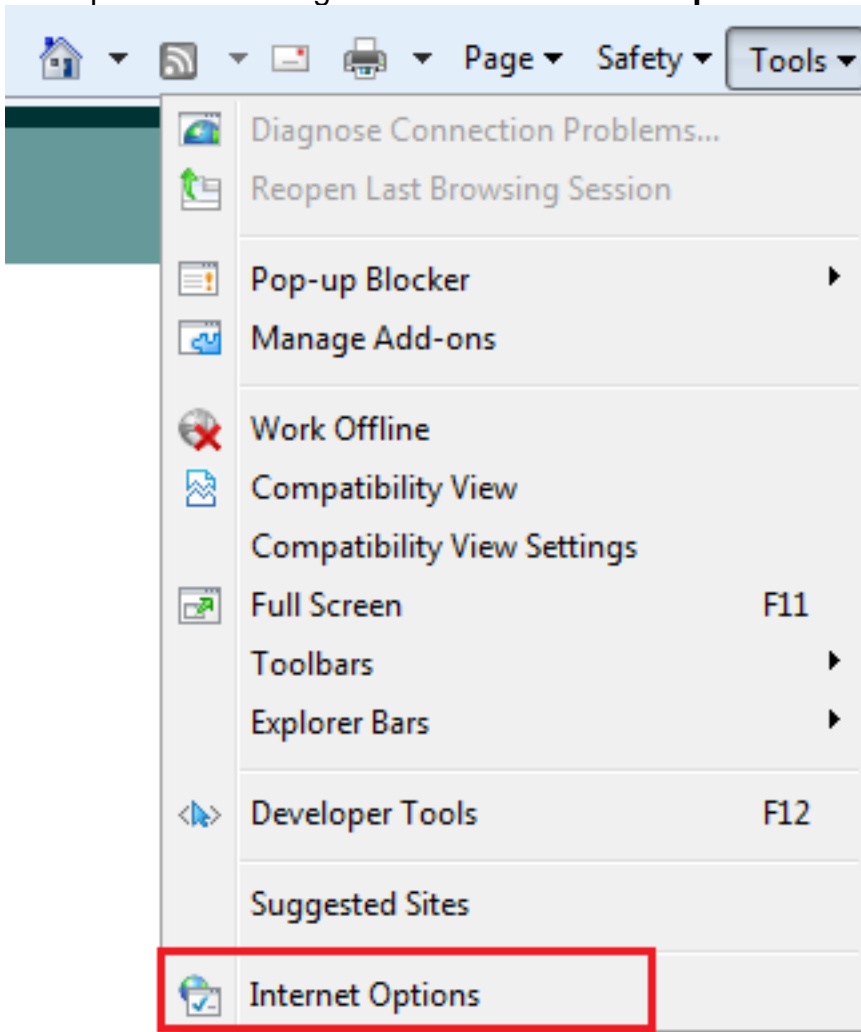
Learn more about [certificate stores](#)

< Back Next > Cancel

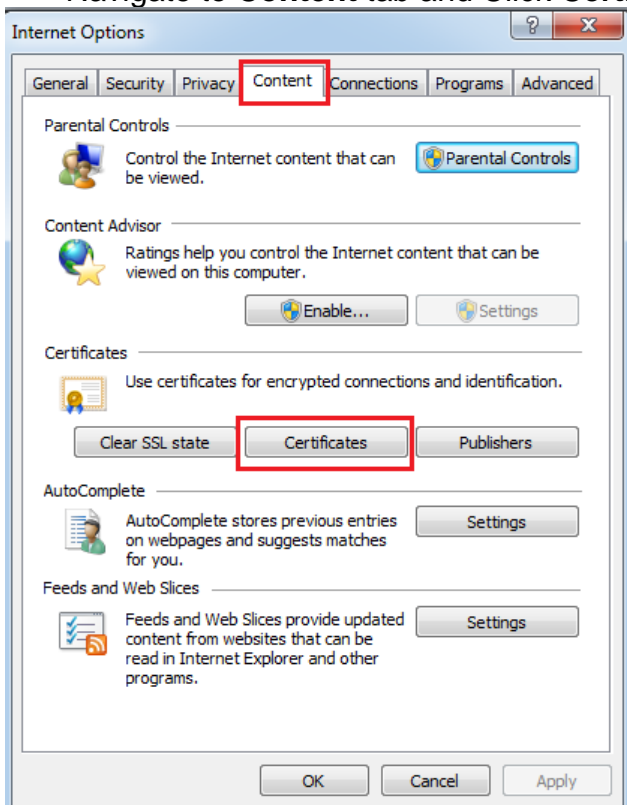
- Click **Finish** in order to complete the installation.



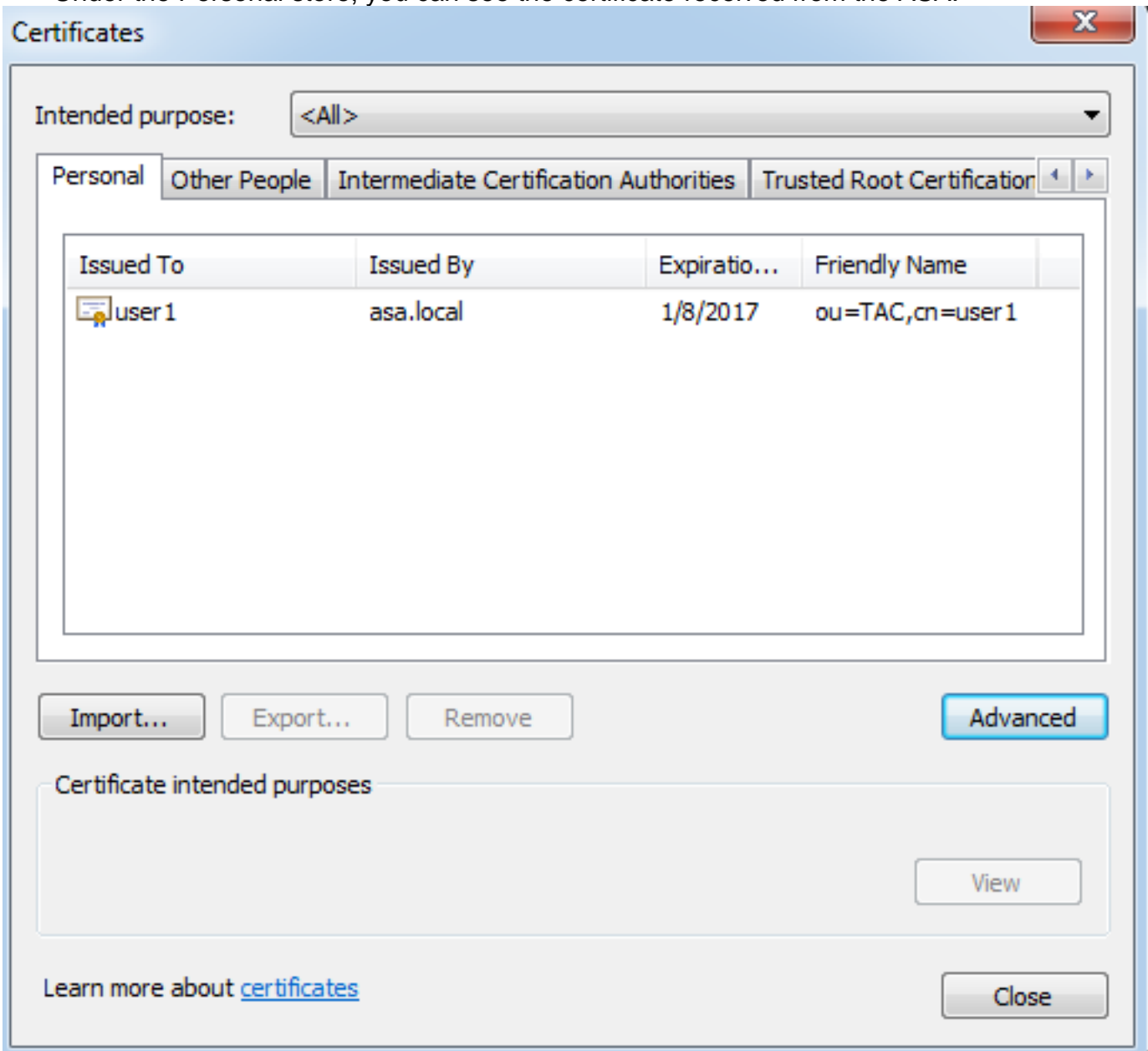
- Once the certificate is successfully installed, you can verify it.
- Open IE and navigate to **Tools > Internet Options**.



- Navigate to **Content** tab and Click **Certificates**, as shown in this image.



- Under the Personal store, you can see the certificate received from the ASA.



ASA as a SSL gateway for AnyConnect Clients

ASDM AnyConnect Configuration Wizard

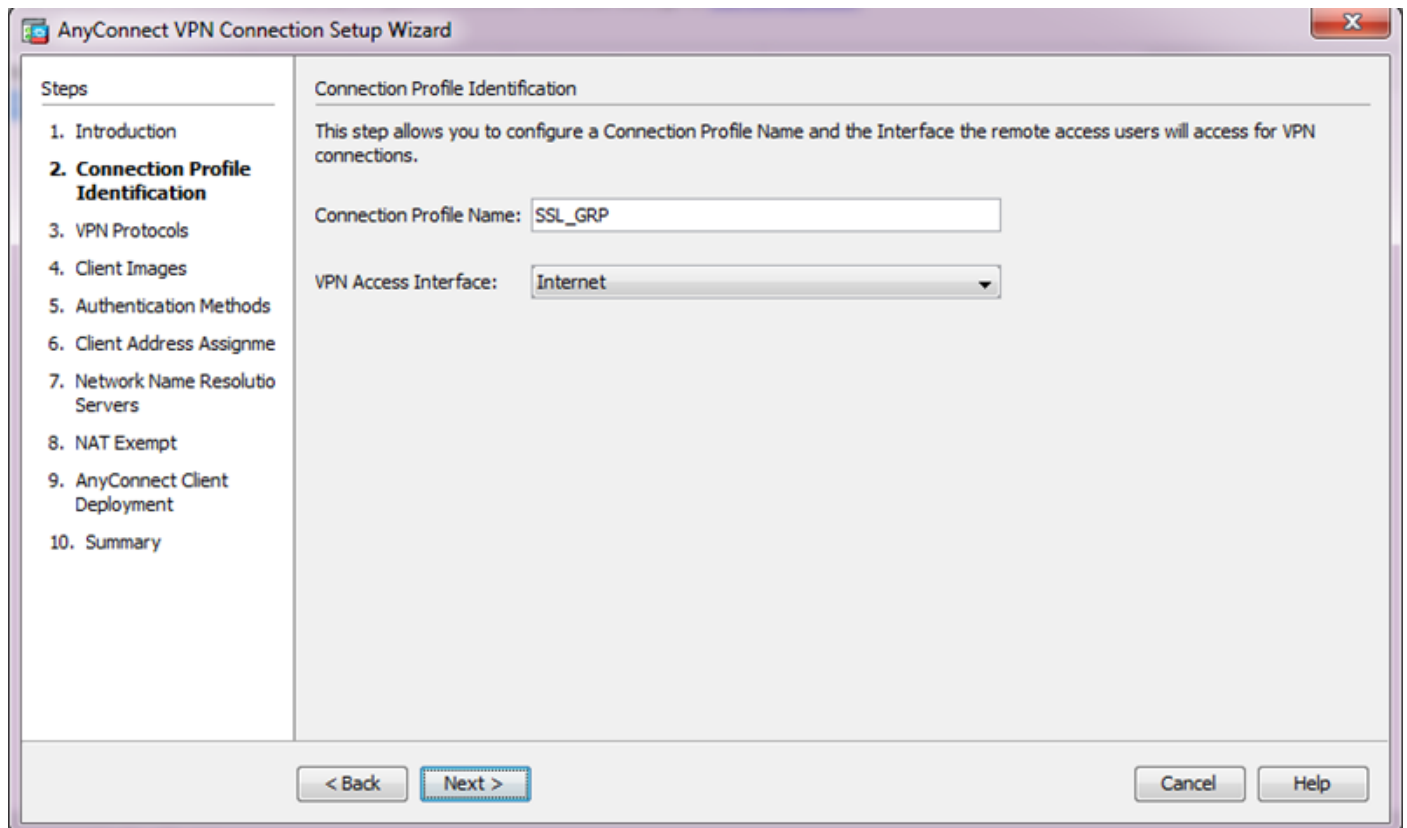
The AnyConnect Configuration Wizard/CLI can be used in order to configure the AnyConnect Secure Mobility Client. Ensure that an AnyConnect client package has been uploaded to the flash/disk of the ASA Firewall before you proceed.

Complete these steps in order to configure the AnyConnect Secure Mobility Client via the Configuration Wizard:

1. Log into ASDM and navigate to **Wizards> VPN Wizards > AnyConnect VPN Wizard** to launch the Configuration Wizard and Click **Next**.



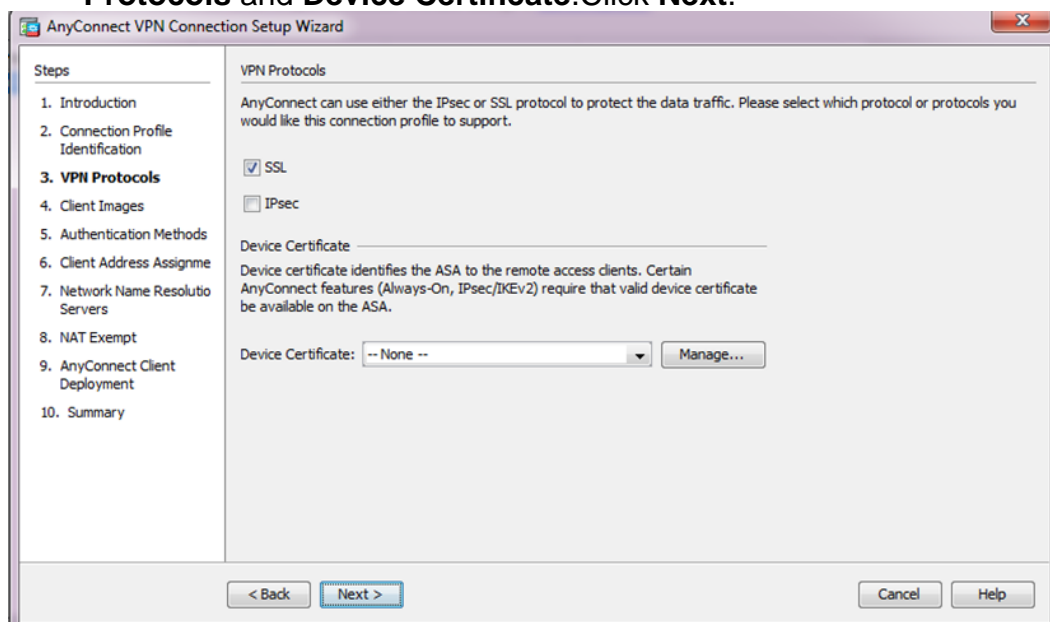
2. Enter the Connection Profile Name, choose the interface on which the VPN will be terminated from the VPN Access Interface drop down menu, and Click **Next**.



The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window at the 'Connection Profile Identification' step. The left sidebar lists steps 1 through 10, with step 2, 'Connection Profile Identification', highlighted. The main area contains the following text: 'This step allows you to configure a Connection Profile Name and the Interface the remote access users will access for VPN connections.' Below this, there is a text input field for 'Connection Profile Name' containing 'SSL_GRP' and a dropdown menu for 'VPN Access Interface' set to 'Internet'. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

3. Check the **SSL** check box in order to enable Secure Sockets Layer (SSL). The Device Certificate can be a trusted third party Certificate Authority (CA) issued certificate (such as Verisign, or Entrust), or a self-signed certificate. If the certificate is already installed on the ASA, then it can be chosen via the drop down menu.

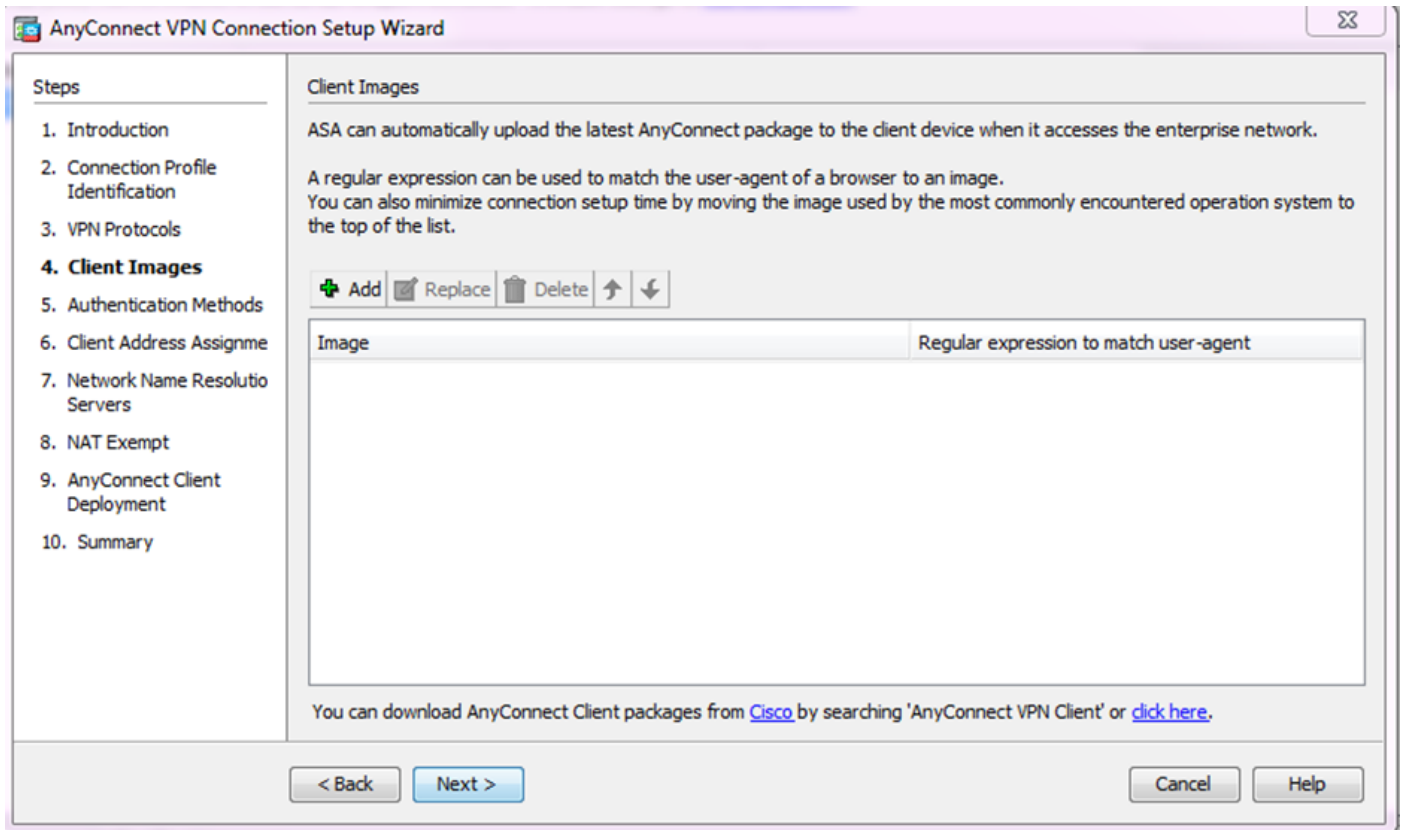
1. **Note:** This certificate is the server-side certificate that will be presented by ASA to SSL clients. If there are no server certificates currently installed on the ASA than a self-signed certificate must be generated, then click **Manage**. In order to install a third-party certificate, complete the steps that are described in the [ASA 8.x Manually Install 3rd Party Vendor Certificates for use with WebVPN Configuration Example](#) Cisco document. Enable the **VPN Protocols and Device Certificate**. Click **Next**.



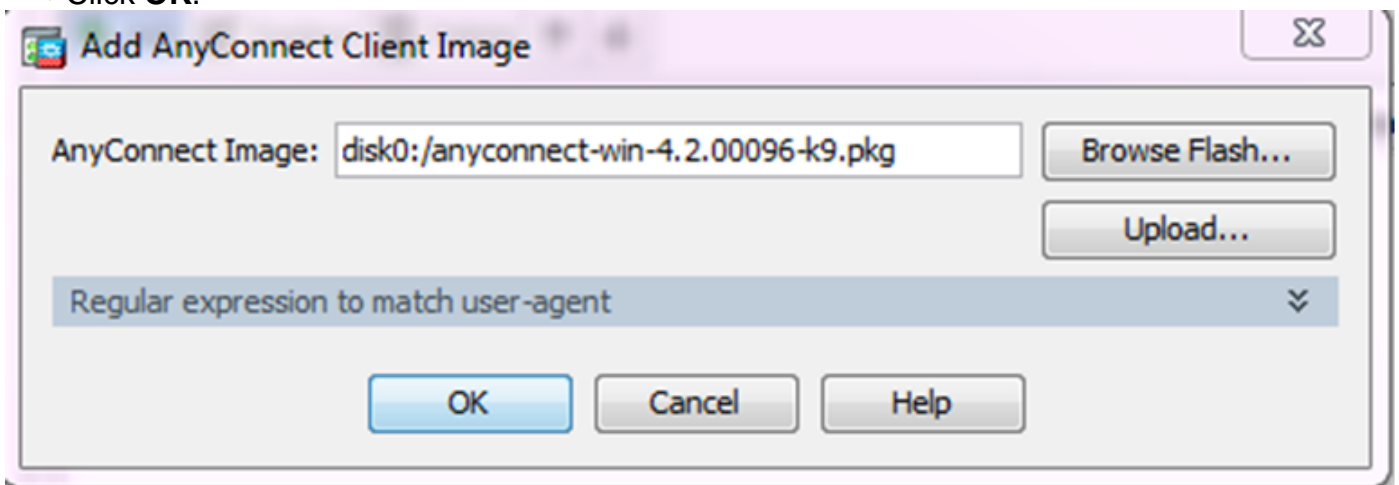
The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window at the 'VPN Protocols' step. The left sidebar lists steps 1 through 10, with step 3, 'VPN Protocols', highlighted. The main area contains the following text: 'AnyConnect can use either the IPsec or SSL protocol to protect the data traffic. Please select which protocol or protocols you would like this connection profile to support.' Below this, there are two checkboxes: 'SSL' (checked) and 'IPsec' (unchecked). Further down, there is a section for 'Device Certificate' with the text: 'Device certificate identifies the ASA to the remote access clients. Certain AnyConnect features (Always-On, IPsec/IKEv2) require that valid device certificate be available on the ASA.' Below this text is a dropdown menu for 'Device Certificate' set to '-- None --' and a 'Manage...' button. At the bottom, there are buttons for '< Back', 'Next >', 'Cancel', and 'Help'.

4. Click **Add** in order to add the AnyConnect Client Package (.pkg file) from the local drive or from the flash/disk of ASA.

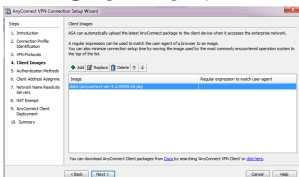
Click **Browse Flash** in order to add the image from the flash drive, or click **Upload** in order to add the image from the local drive of host machine.



- You could upload the AnyConnect.pkg file either from ASA Flash/Disk(if the package is already there) or from the local drive.
- Browse flash – to select the AnyConnect package from the ASA Flash/Disk.
- Upload – to select the AnyConnect package from Local drive of host machine.
- Click **OK**.

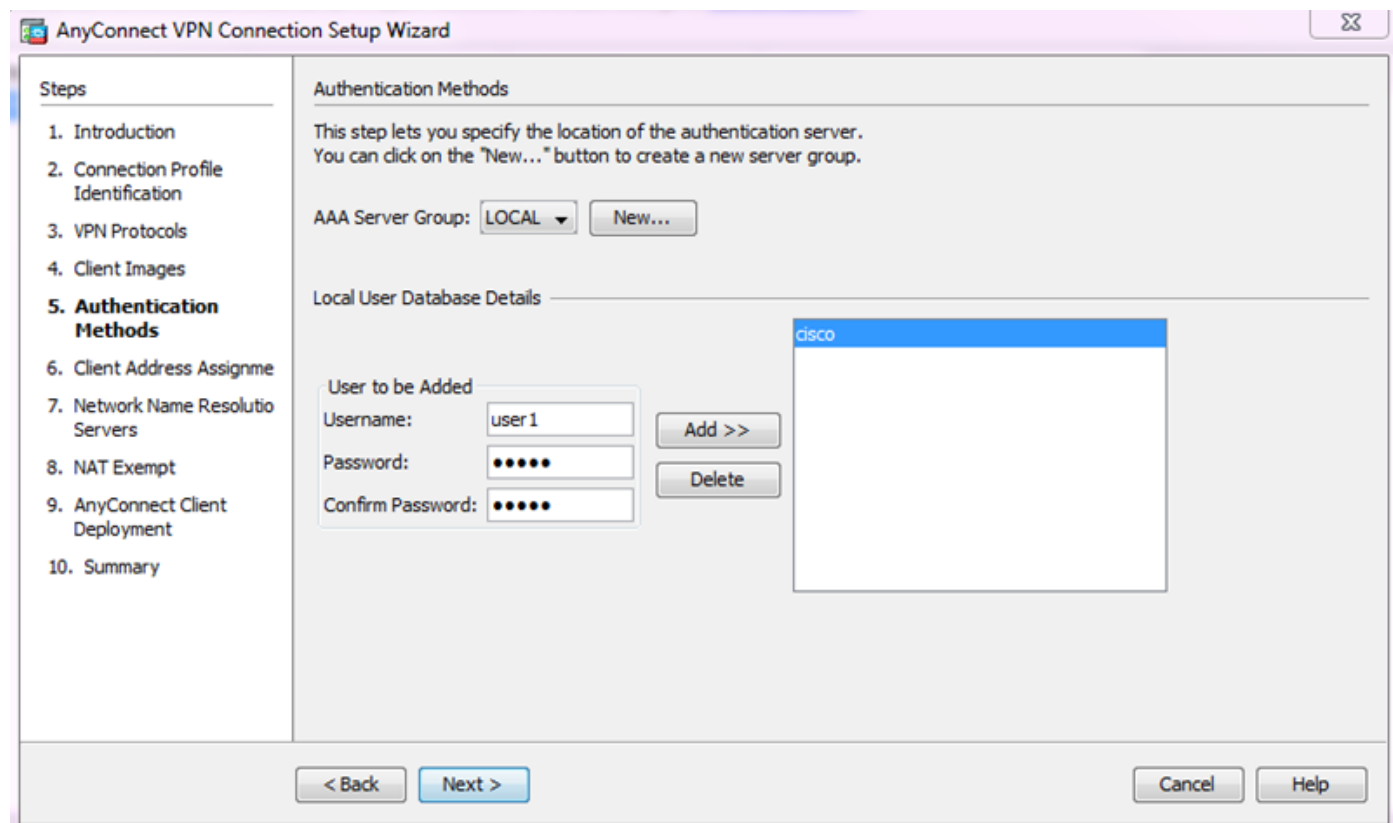


- Click **Next**.

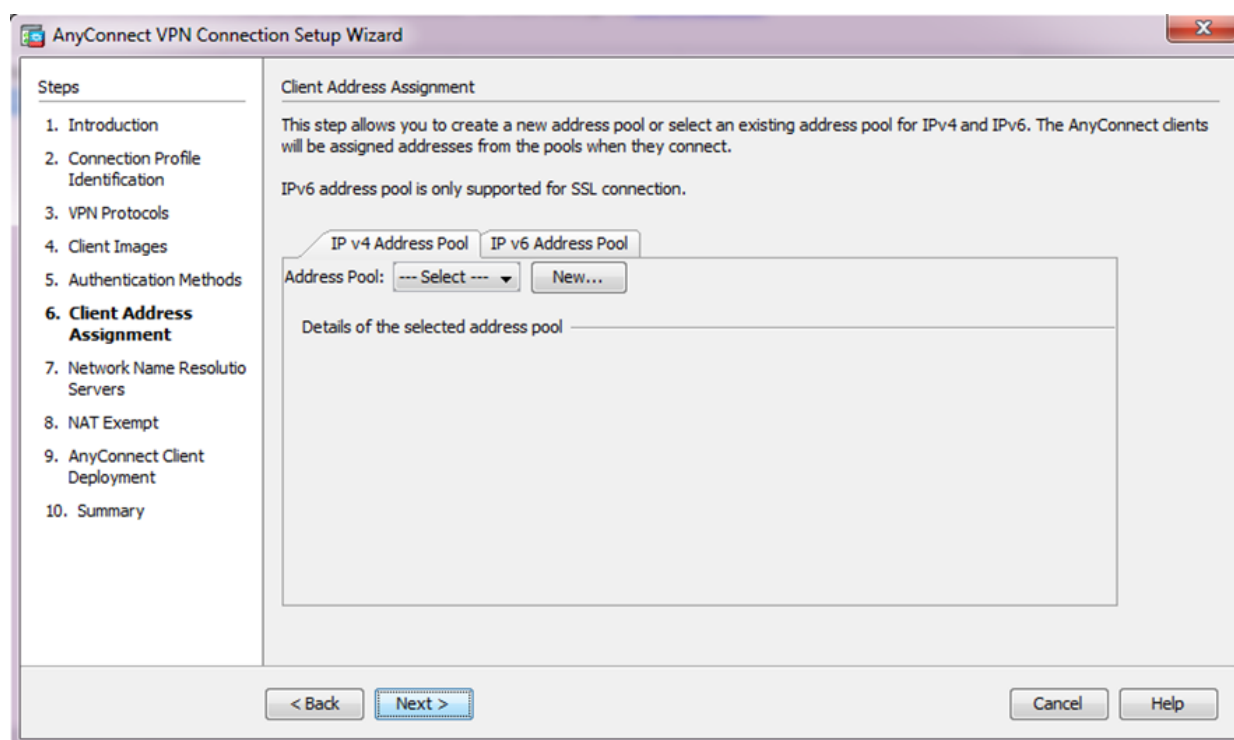


5. The user authentication can be completed via the Authentication, Authorization, and Accounting (AAA) server groups. If the users are already configured, then choose **LOCAL** and Click **Next**. Else add a user to the Local User Database and click **Next**.

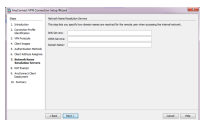
Note: In this example, **LOCAL** authentication is configured, which means that the local user database on the ASA will be used for authentication.



6. Ensure that the Address Pool for the VPN clients is configured. If an ip pool is already configured then select it from the drop down menu. If not, Click **New** in order to configure. Once complete, Click **Next**.



7. Optionally, configure the Domain Name System (DNS) servers and DNS into the DNS and Domain Name fields, and then Click **Next**.



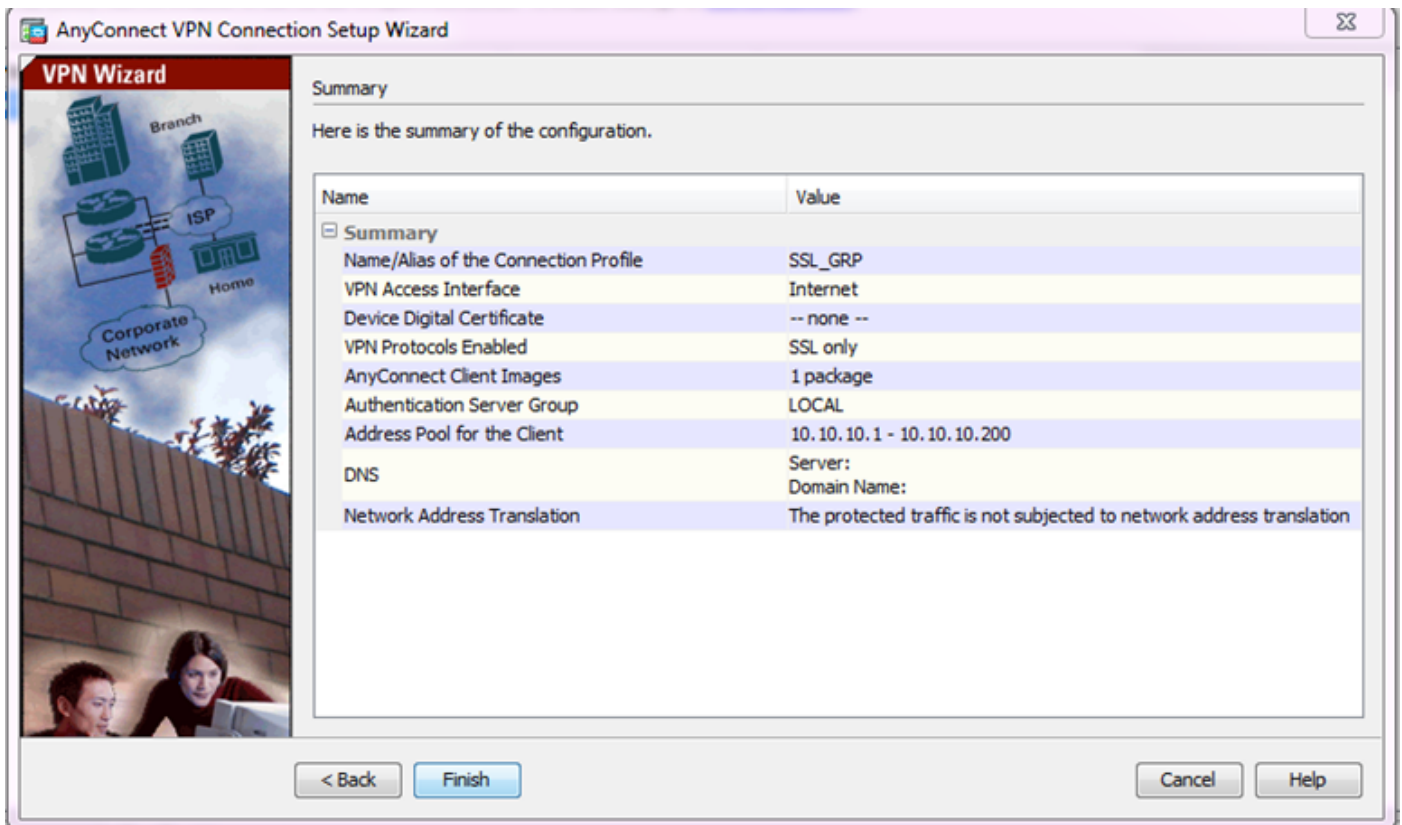
8. Ensure that the traffic between the client and the inside subnet must be exempt from any dynamic Network Address Translation (NAT). Enable the **Exempt VPN traffic from network address translation** check box and configure the LAN interface that will be used for the exemption. Also, specify the Local Network which must be exempted and Click **Next**.

The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window at the 'NAT Exempt' step. The left sidebar lists steps 1 through 10, with '8. NAT Exempt' highlighted. The main area contains the following text: 'If network address translation is enabled on the ASA, the VPN traffic must be exempt from this translation.' Below this is a checked checkbox labeled 'Exempt VPN traffic from network address translation'. Further down, it says 'Inside Interface is the interface directly connected to your internal network.' followed by a dropdown menu for 'Inside Interface' set to 'Inside'. Then, it says 'Local Network is the network address(es) of the internal network that client can access.' followed by a text field for 'Local Network' containing '192.168.10.0/24'. At the bottom, there is a summary sentence: 'The traffic between AnyConnect client and internal network will be exempt from network address translation.' Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

9. Click **Next**.

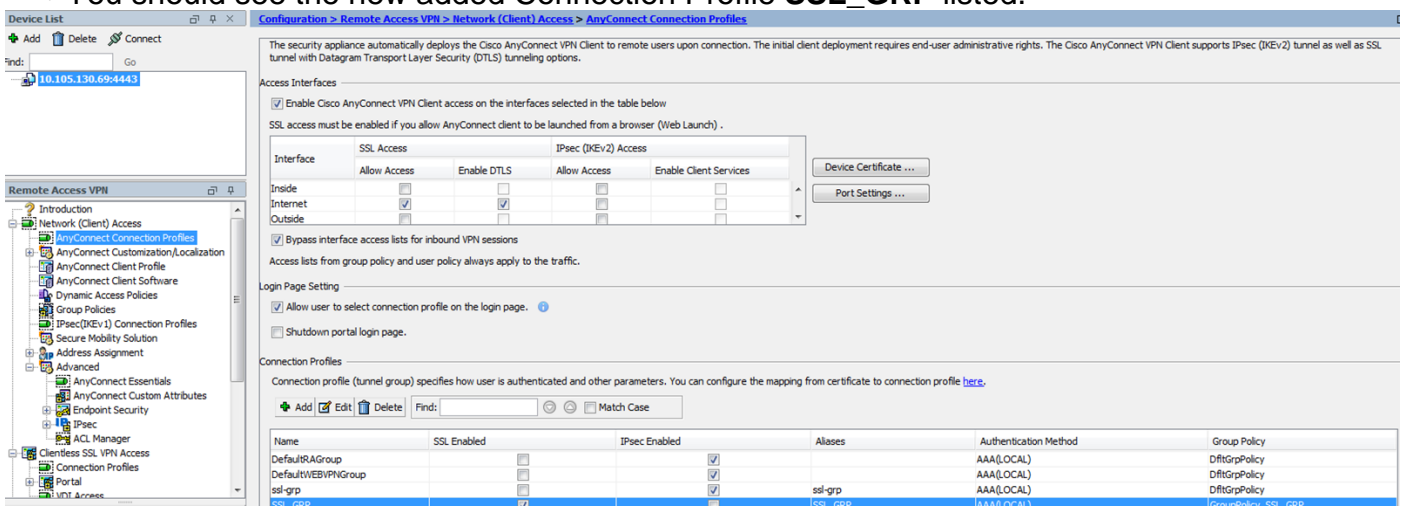
The screenshot shows the 'AnyConnect VPN Connection Setup Wizard' window at the 'AnyConnect Client Deployment' step. The left sidebar lists steps 1 through 10, with '9. AnyConnect Client Deployment' highlighted. The main area contains the following text: 'AnyConnect client program can be installed to a client device by one of the following two methods:' followed by a numbered list: '1) Web launch - On accessing the ASA using a Web Browser, the AnyConnect client package will be automatically installed;' and '2) Pre-deployment - Manually install the AnyConnect client package.' Navigation buttons at the bottom include '< Back', 'Next >', 'Cancel', and 'Help'.

10. The final step shows the summary, Click **Finish** to complete the set-up.



The AnyConnect Client configuration is now complete. However, when you configure AnyConnect via the Configuration Wizard, it configures the **authentication method as AAA** by default. In order to authenticate the clients via certificates and username/password, the tunnel-group (Connection Profile) must be configured to use certificates and AAA as the authentication method.

- Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.
- You should see the new added Connection Profile **SSL_GRP** listed.



- In order to configure **AAA** and **Certificate Authentication**, select the Connection Profile **SSL_GRP** and click **Edit**.
- Under Authentication Method, select **Both**.



Configure CLI for AnyConnect

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

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

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

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

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

*****Configure WebVPN*****

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

```
username user1 password mb02jYs13AXlIAGa encrypted privilege 2
```

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

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

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

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

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

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

Verify

Use this section in order to confirm that your configuration works properly.

Note: The [Output Interpreter Tool](#) ([registered](#) customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

Ensure that the CA server is enabled.

show crypto ca server

```
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!!

Ensure that the user is allowed for enrollment after adding:

*****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
```

You may check the details of the anyconnect connection either via **CLI** or **ASDM**.

Via CLI

show vpn-sessiondb detail anyconnect

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

Session Type: AnyConnect Detailed

```
Username      : user1                      Index      : 1
Assigned IP   : 10.10.10.1                 Public IP   : 10.142.189.181
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Essentials
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx      : 13822                      Bytes Rx    : 13299
Pkts Tx       : 10                        Pkts Rx     : 137
Pkts Tx Drop  : 0                         Pkts Rx Drop : 0
Group Policy  : GroupPolicy_SSL_GRP        Tunnel Group : SSL_GRP
Login Time    : 19:19:10 UTC Mon Jan 11 2016
Duration      : 0h:00m:47s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                       VLAN        : none
```

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

AnyConnect-Parent:

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

SSL-Tunnel:

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

DTLS-Tunnel:

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

NAC:

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

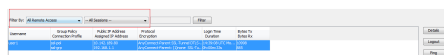
Via ASDM

- Navigate to **Monitoring > VPN > VPN Statistics > Sessions**.
- Choose the **Filter By** as **All Remote Access**.
- You may perform either of the actions for the selected AnyConnect Client.

Details- Provide more information about session

Logout- To manually logout the user from Headend

Ping- To ping the AnyConnect client from the Headend



Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

Caution: On the ASA, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs might increase. Do this with caution, especially in production environments.

- **debug crypto ca**
- **debug crypto ca server**
- **debug crypto ca messages**
- **debug crypto ca transactions**
- **debug webvpn anyconnect**

This debug output shows when the CA server is Enabled using the **no shut** command.

```
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!

This debug output shows client's enrollment

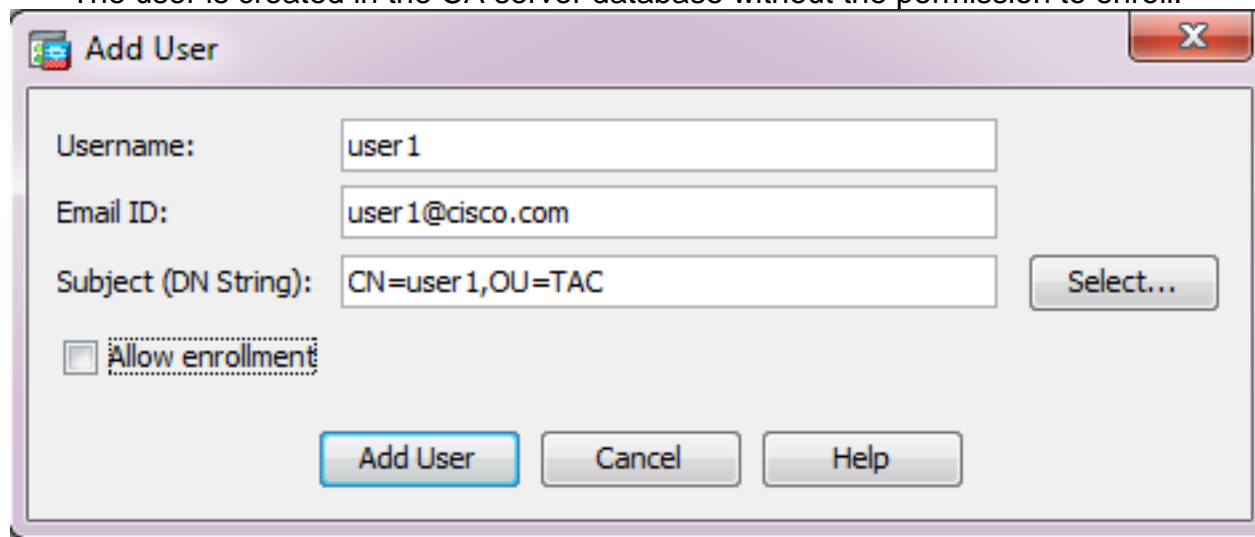
```
ASA# debug crypto ca 255  
ASA# debug crypto ca server 255  
ASA# debug crypto ca message 255  
ASA# debug crypto ca transaction 255
```

```
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
```

The Enrollment of the Client may fail under these conditons:

Scenario 1.

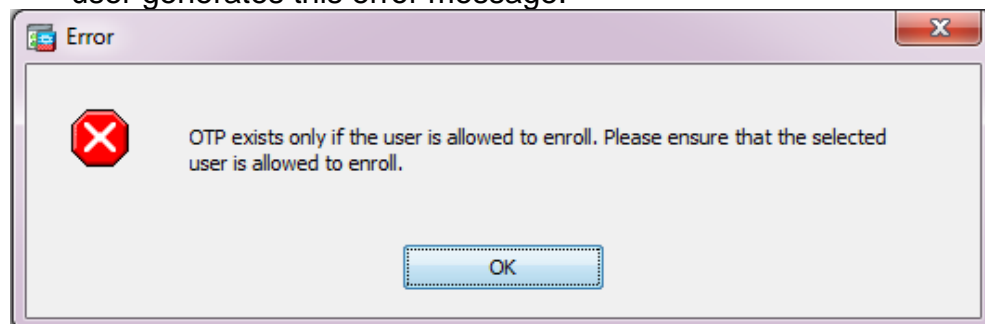
- The user is created in the CA server database without the permission to enroll.



CLI Equivalent:

```
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
```

- In the case where the user is not allowed to enroll, trying to generate/email the OTP for the user generates this error message.



Scenario 2.

- Verify the port and interface on which the enrollment portal is available using the **show run webvpn** command. **The default port is 443** but can be modified.
- Ensure that the client has network reachability to the **IP address of the Interface** on which **webvpn** is enabled on the port used to successfully access the enrollment portal.

The client may fail to access the enrollment portal of ASA in these cases:

1. If any intermediate device blocks the incoming connections from the client to the **webvpn** IP of the ASA on the port specified.
 2. The state of the interface is down on which **webvpn** is enabled.
- This output shows that the enrollment portal is available at the **IP address of the interface Internet** on custom **port 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
```

Scenario 3.

- The default location of CA Server Database Storage is Flash memory of the ASA.
- Ensure that flash memory has free space to generate and save **pkcs12** file for the user during enrollment.
- In the case where flash memory does not have enough free space, ASA fails to complete the client's enrollment process and generates these debug logs:

```
ASA(config)# debug crypto ca 255
ASA(config)# debug crypto ca server 255
ASA(config)# debug crypto ca message 255
ASA(config)# debug crypto ca transaction 255
ASA(config)# debug crypto ca trustpool 255
CRYPTO_CS: writing serial number 0x2.
CRYPTO_CS: file opened: flash:/LOCAL-CA-SERVER/LOCAL-CA-SERVER.ser
CRYPTO_CS: Writing 32 bytes to ser file
CRYPTO_CS: Generated and saving a PKCS12 file for user user1
at flash:/LOCAL-CA-SERVER/user1.p12

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

CRYPTO_CS: Failed to generate pkcs12 file for user user1 status: -1.

CRYPTO_CS: Failed to process enrollment in-line for user user1. status: -1
```

Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [AnyConnect VPN Client Troubleshooting Guide - Common Problems](#)
- [Managing, Monitoring, and Troubleshooting AnyConnect Sessions](#)
- [Technical Support & Documentation - Cisco Systems](#)