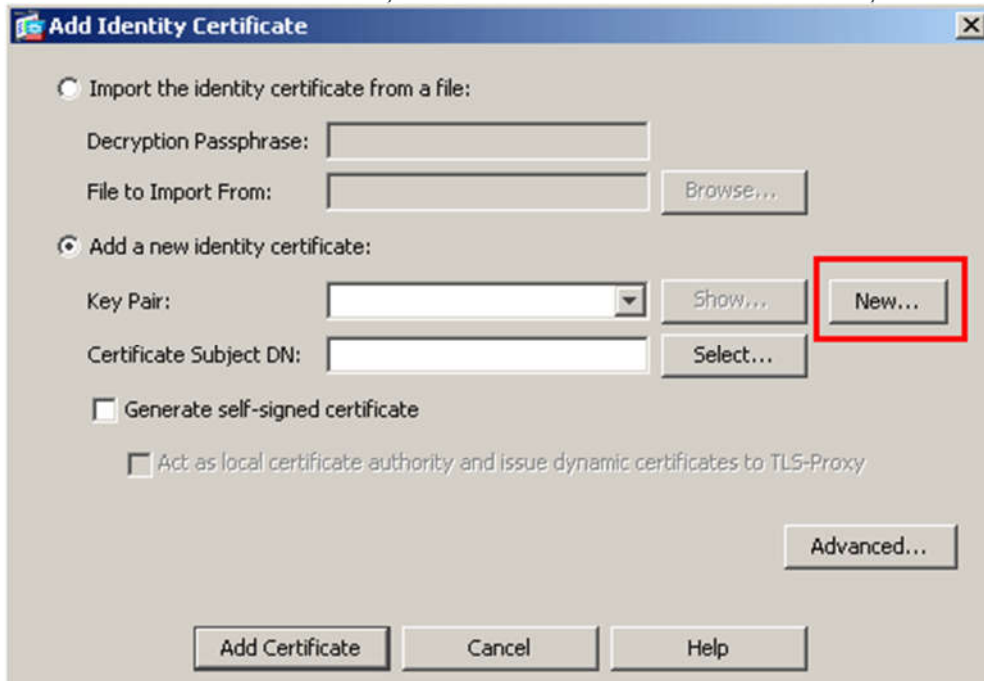


CSR Creation and Install SSL Certificate in Cisco ASA 5500

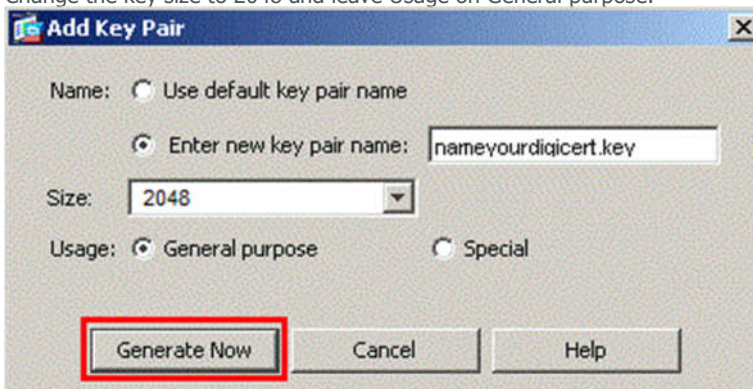
How to generate a CSR in Cisco ASA 5500 SSL VPN/Firewall

1. From the Cisco Adaptive Security Device Manager (ASDM), select "Configuration" and then "Device Management."
2. Expand "Certificate Management," then select "Identity Certificates," and then "Add."
3. Select the button to "Add a new identity certificate" and click the "New..." link for the Key Pair.



The screenshot shows the 'Add Identity Certificate' dialog box. The 'Add a new identity certificate' option is selected. The 'Key Pair' dropdown menu is empty, and the 'New...' button is highlighted with a red rectangle. Other fields include 'Decryption Passphrase', 'File to Import From', 'Certificate Subject DN', and 'Generate self-signed certificate'. There is also an 'Advanced...' button at the bottom right.

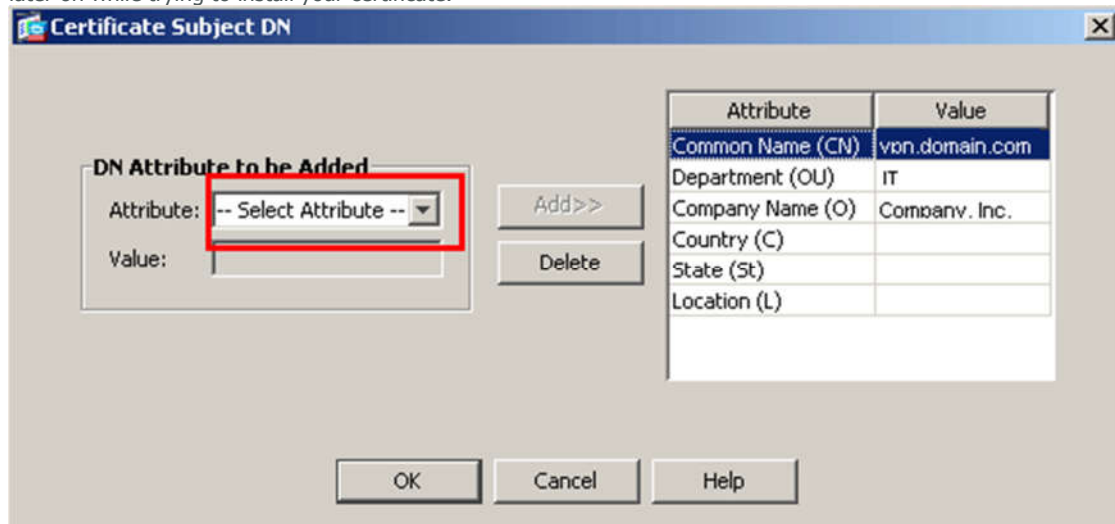
- 4.
5. Select the option to "Enter new key pair name" and enter a name (any name) for the key pair. Next, click the "Generate Now" button to create your key pair.
6. Change the key size to 2048 and leave Usage on General purpose.



The screenshot shows the 'Add Key Pair' dialog box. The 'Enter new key pair name' option is selected, and the name 'nameyourdigicert.key' is entered. The 'Size' dropdown is set to '2048'. The 'Usage' is set to 'General purpose'. The 'Generate Now' button is highlighted with a red rectangle.

- 7.
8. Next you will define the "Certificate Subject DN" by clicking the Select button to the right of that field. In the Certificate Subject DN window, configure the following values by selecting each from the "Attribute" drop-down list, entering the appropriate value, and clicking "Add."
9. **CN** - The name through which the firewall will be accessed (usually the fully-qualified domain name, e.g., vpn.domain.com).
10. **OU** - The name of your department within the organization (frequently this entry will be listed as "IT," "Web Security," or is simply left blank).
 - - The legally registered name of your organization/company.

11. **C** - If you do not know your country's two digit code, find it on our list.
12. **ST** - The state in which your organization is located.
13. **L** - The city in which your organization is located.
14. Please note: None of the above fields should exceed a 64 character limit. Exceeding that limit could cause problems later on while trying to install your certificate.

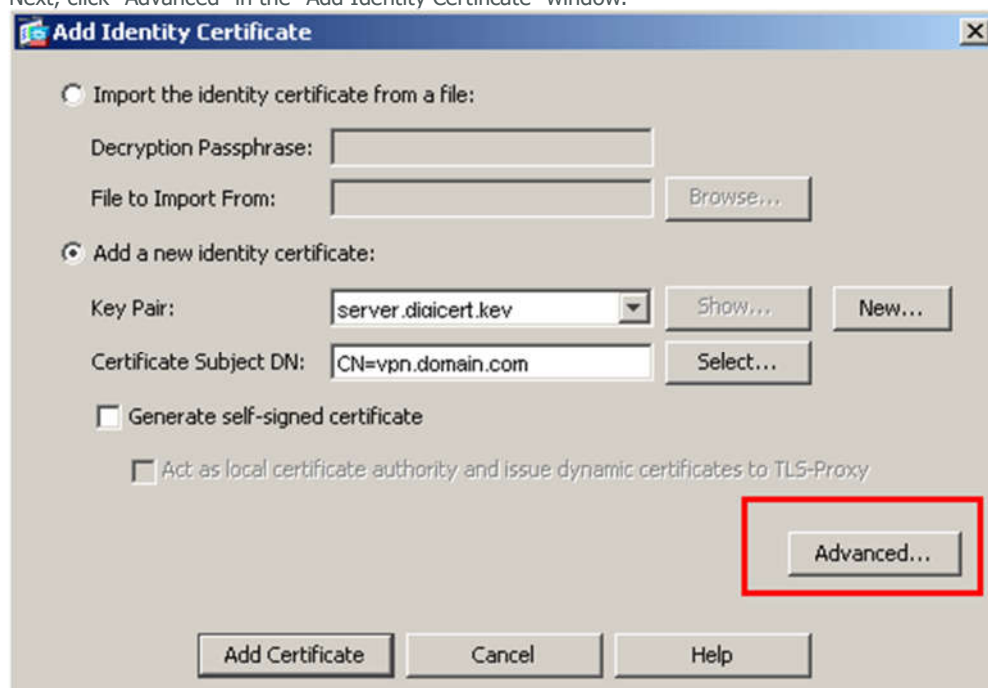


The "Certificate Subject DN" dialog box is shown. It has a title bar with a close button. On the left, there is a section titled "DN Attribute to be Added" with a label "Attribute:" and a dropdown menu showing "-- Select Attribute --". Below it is a "Value:" text field. To the right of this section are "Add>>" and "Delete" buttons. On the far right is a table with two columns: "Attribute" and "Value". The table contains the following entries:

Attribute	Value
Common Name (CN)	vpn.domain.com
Department (OU)	IT
Company Name (O)	Company, Inc.
Country (C)	
State (St)	
Location (L)	

At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

- 15.
16. Next, click "Advanced" in the "Add Identity Certificate" window.



The "Add Identity Certificate" dialog box is shown. It has a title bar with a close button. There are two radio buttons: "Import the identity certificate from a file:" and "Add a new identity certificate:". The "Add a new identity certificate:" option is selected. Below the radio buttons are several fields and buttons:

- "Decryption Passphrase:" text field
- "File to Import From:" text field with a "Browse..." button
- "Key Pair:" dropdown menu showing "server.dioicert.key" with "Show..." and "New..." buttons
- "Certificate Subject DN:" text field showing "CN=vpn.domain.com" with a "Select..." button
- A checkbox labeled "Generate self-signed certificate" which is unchecked.
- A checkbox labeled "Act as local certificate authority and issue dynamic certificates to TLS-Proxy" which is unchecked.
- An "Advanced..." button, which is highlighted with a red rectangle.

At the bottom are "Add Certificate", "Cancel", and "Help" buttons.

- 17.
18. In the FQDN field, type in the fully-qualified domain name through which the device will be accessed externally, e.g., vpn.domain.com (or the same name as was entered in the CN value in step 5).
19. Click "OK" and then "Add Certificate." You will then be prompted to save your newly created CSR information as a text file (.txt extension).

Remember the filename that you choose and the location to which you save it. You will need to [send this file](#) as a text file to us for our process.

Installing your SSL Certificate in the Adaptive Security Device Manager (ASDM)

1. Copy your Intermediate and Primary Certificate files (the IntermediateCA.crt and your_domainname_com.crt) to the directory where you will keep your certificate files.
2. In ASDM select "Configuration" and then "Device Management."
3. Expand "Certificate Management" and select "CA Certificates" and then "Add."
4. With the option selected to "Install from a file," browse to the IntermediateCA.crt file and then click the "Install Certificate" button at the bottom of the "Install Certificate" window.
5. Your Intermediate (or chain) certificate file is now installed. You will now need to install the your_domainname_com.crt file.
6. In ASDM select "Configuration" and then "Device Management."
7. Expand "Certificate Management" and select "Identity Certificates."
8. Select the appropriate identity certificate from when your CSR was generated (the "Issued By" field should show as not available and the "Expiry Date" field will show Pending...). Click the Install button.
9. Browse to the appropriate identity certificate (the your_domainname_com.crt) and click "Install Certificate."

At this point you should receive confirmation that the certificate installation was successful.

Configuring WebVPN with ASDM to Use the New SSL Certificate

1. In ASDM select "Configuration" and then "Device Management."
2. Click "Advanced" and then "SSL Settings."
3. From "Certificates," choose the interface used to terminate WebVPN sessions, and then choose "Edit."
4. From the "Certificate" drop-down, select the newly installed certificate, then "OK," and then "Apply."
5. Configuring your certificate for use with the selected kind of WebVPN session is now complete.

SSL Certificate Installation from the Cisco ASA command line (alternate installation method)

1. From the ciscoasa(config)# line, enter the following text:
2. *crypto ca authenticate my.digicert.trustpoint*
3. Where my.digicert.trustpoint is the name of trustpoint created when your certificate request was generated.
4. Next, enter the entire body of the IntermediateCA.crt file followed by the word "quit" on a line by itself (the IntermediateCA.crt file can be opened and edited with a standard text editor, and the entire body of that file should be entered when prompted).
5. When asked to accept the certificate, enter "yes".
6. When the certificate has been successfully imported, enter "exit".
7. Your Intermediate (or chain) certificate file is now installed. You will now need to install the your_domainname_com.crt file.
8. From the ciscoasa(config)# line, enter the following text:
9. *crypto ca import my.digicert.trustpoint certificate*
10. Where my.digicert.trustpoint is the name of trustpoint created when your certificate request was generated.
11. Next, enter the entire body of the your_domainname_com.crt file followed by the word "quit" on a line by itself (the your_domainname_com.crt file can be opened and edited with a standard text editor, and the entire body of that file should be entered when prompted).
12. You should then receive a message that the certificate was successfully imported.

Configuring WebVPN to Use the New SSL Certificate from the Cisco ASA command line

1. From the ciscoasa(config)# line, enter the following text:
ssl trust-point my.digicert.trustpoint outside wr mem
 - a. Where my.digicert.trustpoint is the name of trustpoint created when your certificate request was generated and "outside" is the name of the interface being configured.
 - b. Make sure to save the configuration.