Article Number: 1479 | Rating: 1/5 from 1 votes | Last Updated: Wed, Dec 2, 2020 at 7:55 PM

Before you request a certificate, use the Cisco Adaptive Security Device Manager (ASDM) to generate a Certificate Signing Request (CSR) for your Cisco Adaptive Security Appliance (ASA) 5500 VPN or firewall. Launch theÂ **Cisco ASDM (Adaptive Security Device Manager)**. In the list of icons near the top of the screen, clickÂ **Configuration**. On the left hand sidebar, clickÂ **Remote Access VPN**. In the new panel on the left, click to expandÂ **Certificate Management**Â then clickÂ **Identity Certificates**. On the right-hand side of the main panel, clickÂ **Add**. For theÂ **Trustpoint Name**, simply enter a name to easily identify your SSL at a later date. Select the radio button toÂ **Add a new identity certificate**. To the right ofÂ **Key Pair**, clickÂ **New...**. On the new window, selectÂ **RSA**Â forÂ **Key Type**. Select the radio button forÂ **Enter new key pair name**Â and enter a name to easily identify your SSL at a later date. WithÂ **Size**, selectÂ **2048**Â in the drop down menu. ForÂ **Usage**, selectÂ **General purpose**. ClickÂ **Generate Now**. Back on theÂ **Add Identity Certificate**Â window, clickÂ **Select...**Â to the right ofÂ **Certificate Subject DN**. In the new window, you'll want to include your attributes by choosing an option from theÂ **Attribute**Â drop down menu, typing in theÂ **Value**Â and clickingÂ **Add>>**Â for each item below:

Attribute	Description
Common Name (CN)	The fully-qualified domain name, or URL, you want to secure for connections to your firewall. *Note:*Â If you're requesting a Wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard, for example *.coolexample.com.
Company Name (O)	The legally-registered name for your business. If you're enrolling as an individual, enter the certificate requestor's name.

1. ClickÂ **OK**Â to confirm.
2. Back on theÂ **Add Identity Certificate**Â window, clickÂ **Advanced...**.
3. In the new window, fill out the field forÂ **FQDN**Â with the sameÂ **Common Name (CN)**Â you used earlier.

4. ClickÂ **OK**Â to confirm.
5. Back on theÂ **Add Identity Certificate**Â window, ensure theÂ **Enable CA flag in basic constraints extension**Â remains checked.
6. ClickÂ **Add Certificate**.
7. In the prompt to save your CSR, clickÂ **Browse...**.
8. Choose a location where you wish to save the CSR with theÂ `.txt`Â extension at the end of your file name. You'll need to open this newly created file to copy its contents for the next step.

Note:Â As a courtesy, we provide information about how to use certain third-party products, but we do not endorse or directly support third-party products and we are not responsible for the functions or reliability of such products. Third-party marks and logos are registered trademarks of their respective owners. All rights reserved.

Posted - Wed, Dec 2, 2020 at 7:55 PM.

Online URL:

https://www.heartinternet.uk/support/article/generate-a-csr-certificate-signing-request-for-my-cisco-asa-5500-vpn-fire