# AnyConnect Certificate for VPN

To setup your system to use certificate based authentication with AnyConnect:

1. Generate a system certificate request and key matching your system's FQDN

**Generating the CSR and key with a hostname of 2yd3hm2**

openssl req -out 2yd3hm2.csr -new -newkey rsa:2048 -nodes -keyout 2yd3hm2.key

Generating a 2048 bit RSA private key

...................................+++

......................................................................+++

writing new private key to '2yd3hm2.key'

-----

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

-----

Country Name (2 letter code) [XX]:US

State or Province Name (full name) []:Nevada

Locality Name (eg, city) [Default City]:Las Vegas

Organization Name (eg, company) [Default Company Ltd]:Allegiant Air

Organizational Unit Name (eg, section) []:LinuxSE

Common Name (eg, your name or your server's hostname) []:2yd3hm2.authentication.allegiantair.com

Email Address []:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []

1. Send the CSR file to the Windows team for them to sign it with their CA
2. You will need the signed certificate from Windows, the CA certificate, and your private key to setup the AnyConnect client
3. Rename the signed certificate file to have a .pem extension and the key file to have .key
4. Make $HOME/.cisco
5. You will need the following directory structure created under $HOME/.cisco

**Directory tree**

[16:02:48]-[hj1u@2yd3hm2 .cisco]~/.cisco $ ls -lR

.:

total 0

drwxrwxr-x. 4 hj1u hj1u 30 Jun 17 10:05 certificates

./certificates:

total 0

drwxrwxr-x. 2 hj1u hj1u 88 Jun 17 10:11 ca

drwxrwxr-x. 3 hj1u hj1u 41 Jun 17 10:08 client

./certificates/ca:

total 4

-rw-rw-r--. 1 hj1u hj1u 1306 Jun 17 10:07 CACERT.pem

./certificates/client:

total 4

-rw-rw-r--. 1 hj1u hj1u 2178 Jun 17 10:08 myclient.pem

drwxrwxr-x. 2 hj1u hj1u 26 Jun 17 10:08 private

./certificates/client/private:

total 4

-rw-rw-r--. 1 hj1u hj1u 1708 Jun 17 10:08 myclient.key

1. Copy the signed system certificate to $HOME/.cisco/certificates/client/myclient.pem
2. Copy the CA certificate to $HOME/.cisco/certificates/ca/CACERT.pem (get the latest AD CA cert from windows eng or pull it yourself)
3. Copy the private key to $HOME/.cisco/certificates/client/private/myclient.key

It is not important that the certificate and key be called "myclient" but they MUST match and MUST end in .pem and .key.

You are now configured to use certificate authentication with the AnyConnect VPN client.

### REFERENCE:

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/214612-configure-anyconnect-secure-mobility-cli.html>