CSR Creation and SSL Installation on Adobe Connect

CSR Creation for Adobe Connect

This is a full walkthrough of how to setup and install Adobe Connect 7 Pro with SSL. If you are having trouble with your CSR creation or SSL installation, hopefully this can clarify any issues you encountered understanding the Adobe documentation.

If you do not have OpenSSL (a common SSL manipulation tool), you will want to download it online before continuing.

Creating CSRs and Private Keys in Adobe Connect 7 Pro

- You will need to create two private keys and certificate signing request files. The easiest way to do this is to use our OpenSSL CSR creation tool. follow the instructions on that page, and make sure to use connect.yourdomain.com as the common name for the first request and connectmeeting.yourdomain.com as the common name for your second request.
- You will have two key files and two CSR files. You will send the CSRs to us along with your certificate orders or reissue requests. Add a .pem extension to your .key files (they should be named connect.yourdomain.com.key.pem and connectmeeting.yourdomain.com.key.pem, respectively).
- Copy your .pem keys from the previous step to Adobe Connect's root install folder. These files will be used for installing your certificates once you receive your signed certificate files back.

SSL Installation in Adobe Connect 7 Pro

You will be able to continue with your certificate installation once your order has been validated and you have received your signed cert files. These will be sent to you in an email, or can be downloaded inside your account by clicking on the order number once the certificates have been issued.

- Open your .pem keys seperately like you would open any text file (you should see an encrypted text string starting with BEGIN and END tags.
- Open the connect_yourdomain_com.crt and connectmeeting_yourdomain_com.crt files that you received back from DigiCert, also as text files.
- Copy and paste the entire text (including begin and end tags) of each certificate file into the respective .key.pem files immediately after (on the next line of text) the END tag of the keys.
- Next open your IntermediateCA.crt file (this will be the same for both certificates) and paste the body of this file at the very bottom of both text files, after the end tags for the server certificates.
- DNS entries for connect.yourdomain.com and connectmeeting.yourdomain.com should be set up already, make sure you do not have any host entries on the server for testing purposes for these two entries before completing your SSL installation.
- Open and backup [path_to\comserv\win32\conf_defaultRoot\Adaptor.xml]. Replace the SSL block (a little more than halfway down) with the following block of text, replacing text in brackets with the information applicable to your configuration:

```
1. <SSL>
   <Edge name="applicationserver">
   <SSLServerCtx>
   <SSLCertificateFile>[<connect install path>\\connect.mydomain.com.key.pem]</SSLCertificateFile>
   <SSLCertificateKeyFile type="PEM">[<connect install
   path>\\connect.mydomain.com.key.pem]</SSLCertificateKeyFile>
   <SSLPassPhrase>mypassphrase</SSLPassPhrase>
   <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
   <SSLSessionTimeout>5</SSLSessionTimeout>
   </SSLServerCtx>
   </Edge>
   <Edge name="meetingserver">
   <SSLServerCtx>
   <SSLCertificateFile>[\\connectmeeting.mydomain.com.key.pem]</SSLCertificateFile>
   <SSLCertificateKeyFile type="PEM">[\\connectmeeting.mydomain.com.cert.cer]</SSLCertificateKeyFile>
   <SSLPassPhrase>mypassphrase</SSLPassPhrase>
   <SSLCipherSuite>ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH</SSLCipherSuite>
   <SSLSessionTimeout>5</SSLSessionTimeout>
   </SSLServerCtx>
   </Edge>
   </SSL>
```

- Find the <HostPortList> node in the same adaptor.xml file. There will probably be a line of uncommented text similar to the following:
    - <HostPort name="edge1">$Unknown macro: {DEFAULT_FCS_HOSTPORT}</HostPort>
- Replace that entire block of text with the following text:
    1. <HostPort name="applicationserver"ctl_channel=":19351">your application server ip:-443</HostPort>
       <HostPort name="meetingserver"ctl_channel=":19350">your meeting server ip:-443</HostPort>
- Next, open [<connect install path>\\custom.ini] and add the following code to the very end of that file:
    1. ADMIN_PROTOCOL= https://\\\\
       SSL_ONLY=yes
       HTTPS_PORT=8443
       RTMP_SEQUENCE=rtmps://external-host:443/?rtmp://localhost:8506/
- Save and close your customer.ini file.
- Now open and backup your VHost.xml file at [<connect install path>\\comserv\\win32\\conf_defaultRoot_defaultVHost_\\VHost.xml]
- Your RouteEntry node should be empty. Find that section and replace it with:
    1. <RouteEntry protocol="rtmp">:;*:$
       Unknown macro: {ORIGIN_PORT}
       </RouteEntry>
       Once you have replaced this section, save and close the VHost.xml file.
- Restart the Adobe Connect Enterprise Server & Adobe Connect Meeting Server services.
- Open the Application Management Console by going to http://localhost:8510/console, and under Server Settings, change the Connect Pro Host to your connect.mydomain.com domain, and the Host Mappings External Name to connectmeeting.mydomain.com.
- Once again, go ahead and restart the Adobe Connect Enterprise Server & Adobe Connect Meeting Server services.

Your Adobe Connect server should now work properly, and force all non-secure traffic over to SSL.