CSR Creation and Installation for C2Net Stronghold

SSL Certificate CSR Generation in C2Net Stronghold Server

1. Certificates and keys are managed with three scripts in Stronghold: genkey, getca and genreq. They are typically stored in **/usr/local/ssl/private/**.
   If you do not already have a key for your server,
   At the prompt, run **genkey** and the name of the host for which you are generating the CSR (i.e., 'genkey yourserver'). This will show two filenames - the key file and CSR file - and display their respective locations.
   If you do already have a key for your server,
   At the prompt, run **genreq**, not **genkey**, to create the CSR only.
   The script will prompt you to be certain you aren't overwriting a previous certificate request and key.

   You will be prompted for the key size in bits - select 2048 bits.

   Then the fun part - when prompted, hit keys randomly. When the script beeps and the counter shows zero, stop. (This random data is used to create a unique public and private key pair.)

   When asked, enter 'y' to proceed. You will be prompted for specific information about your company, your server and your Certified Authority.

   (For your CA, select the option 'Other'.)

   The genkey script will create the CSR automatically. It is highly recommended that you back up your key file and CSR and keep them some place secure. **The key is required to install your certificate**.
2. Please send the CSR file to us for our process.

Installing your C2Net Stronghold SSL Certificate

Installing your Primary Server Certificate (your_domain_name.crt)

1. If you have a temporary SSL Certificate in your /ServerRoot/ssl/certs/ directory, move or delete it.

2. Run Command "**getca servername**" where "servername" is the same name created during generation of your Private-Key or CSR request.
3. Open your Primary Certificate (your_domain_name.crt) with a text editor and copy the content (see example below), to your clipboard:

   -----BEGIN CERTIFICATE-----
   text ...
   -----END CERTIFICATE-----

4. Paste the contents of your Certificate into the getca terminal window and enter Control-D or the appropriate EOF character.

Installing your Intermediate CA Certificate

1. Once you have completed the steps above you will copy your Intermediate CA Certificate to your server in the /ssl/certs/ directory.

2. Locate and edit your **httpd.conf** file (normally located in the **/conf/** directory). Change the SSLCACertificateFile entry in your httpd.conf file so that it points to the Intermediate Root Certificate file as follows:
   SSLCACertificateFile ssl/certs/IntermediateCA.crt
3. Restart your server.