NGINX: Generate CSRs (Certificate Signing Requests)
Article Number: 1351 | Rating: Unrated | Last Updated: Wed, Dec 2, 2020 at 5:13 PM
Before you can request your SSL, you must generate a Certificate Signing Request (CSR) From your server. When you have completed generating your CSR, cut/copy and paste it into the CSR field on the SSL certificate-request page. **To Generate NGINX CSRs** Connect to your server via SSH. Run the following command: openssl req -new -newkey rsa:2048 -nodes -keyoutÂ *your domain name*.key -outÂ *your domain name*.csr **Note:**Â ReplaceÂ *`your domain name`*Â with the domain name you're securing. For example, if your domain name is coolexample.com, you would typeÂ `coolexample.key`Â andÂ `coolexample.csr`. Enter the requested information:

Field	What to enter...
Common Name	The fully-qualified domain name, or URL, you want to secure. If you are requesting a Wildcard certificate, add an asterisk (*) to the left of the common name where you want the wildcard, for exampleÂ **.coolexample.com*.
Organization	The legally-registered name for your business. If you are enrolling as an individual, enter the certificate requestor's name.
Organization Unit	If applicable, enter the DBA (Doing Business As) name.
City or Locality	Name of the city where your organization is registered/located. Do not abbreviate.

-
- Open the CSR in a text editor and copy all of the text.
- Paste the full CSR into the SSL request area in your account.

Posted - Wed, Dec 2, 2020 at 5:13 PM.

Online URL: https://www.heartinternet.uk/support/article/nginx-generate-csrs-certificate-signing-requests.html