# Generating a CSR on Amazon Web Services (AWS)

SSL certificates can be used for some AWS products, such as AWS Elastic Beanstalk, Elastic Load Balancing, CloudFront and AWS OpsWorks. In this article we will describe the process of uploading the certificate in order to use https connection to access your objects in the CloudFront and or updating the certificate for Load Balancer.

The first step of the certificate managing after the purchase is the process of activation. For activation you need to generate the Certificate Signing Request (CSR) through IAM.

Certificate Signing Request is a small encrypted piece of text which contains information about a certificate applicant and the domain name to secure. Once you activate the certificate with the help of CSR, the information passes to the Certificate Authority which validates the certificate based on the information from the CSR.

RSA private key is generated along with the CSR and plays an important role in encrypting the information. It should be stored safely on the server and not be compromised.
The following command-line tools are required for creating and uploading the certificate on AWS:

- ✓ OpenSSL. This tool is designed to generate a private key and CSR.
- ✓ AWS command-line interface (CLI). It is used to upload certificates to AWS.

The openssl command to generate a private key is:

**openssl genrsa 2048 > private-key.pem**

2048 is a key size. The size of the public key cannot exceed 2048 bits in this CSR.

For private-key.pem specify your own key name in order to identify it later during installation.

The CSR is generated based on the private key. The following command is used for the CSR creation:

**openssl req -new -key private-key.pem -out csr.pem**

The output will look similar to the following example:

> *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.*

The following information needs to be filled in. We strongly recommend filling all the fields in. The CSR with any blank fields can be rejected by our system or by the Certificate Authority.

Please use only alphanumeric characters. The CSR with special symbols such as Ä or È will not be recognized. Such special characters should be replaced with their analogs from the alphanumeric: A and E accordingly.

**Country name.** Two-letter abbreviation: Example: US = United States, SE = Sweden, DE = Germany

**State of Province.** Full name of state: Washington

**Locality name.** City name: Seattle

**Organization Name.** Full legal name of your company: Company LLC

***note**: for certificates with domain validation this field is not obligatory and can be replaced with NA

**Organizational Unit.** Additional company information: Sales

***note**: for certificates with domain validation this field is not obligatory and can be replaced with NA

**Common Name.** Fully qualified domain name you need to secure: www.example.com

**Email address.** Server administrator's email address: admin@example.com

***note**: while filling in the Common Name field, it is necessary to remember that it should be the exact domain name you need to secure. It should look like www.example.com, example.com or mail.example.com if you need to secure the subdomain.

For a Wildcard certificate the common name should be stated as *.example.com or *.sub.example.com.

Most certificates we provide secure both www.example.com and example.com automatically. However if you have any doubts, it is recommended to check the correct way of defining your domain name for a particular certificate with our Support Team.

In the output you will see the CSR in plain text. This text should be saved and used for the certificate activation. Once the certificate is issued by the Certificate Authority, you can proceed with its installation.