

# Install your SSL Certificate

The install procedure above initially configures eagle-i with a self-signed certificate; this is acceptable for an **EVALUATION/DEVELOPMENT NODE** environment, but not for a **PRODUCTION NODE** instance. In order to finalize the installation of a production instance, please follow the steps below.

## 1. Transfer certificate, certificate chain and private key to the EC2 instance



These files are security-sensitive. Please make sure they are transferred to you in a secure manner (e.g. a memory stick, or using the `scp` command) and **delete** them from your personal machine once they are installed. If in doubt, please ask for assistance of your IT department.

Obtain, from the person who purchased the certificate, the following files:

- The RSA key used at certificate purchase time and its password, e.g. `key.pem`
- The actual certificate returned by the certificate authority, e.g. `cert.crt`
- The certificate authority's (CA) certificate chain (depending on the particular CA, some of these may need to be downloaded - refer to their documentation), e.g. `ca.crt`

Assuming the files are located in a directory `/my-home/aws/cert` on your machine, here are two methods for securely transferring the files to your EC2 instance:

1. Using a terminal
  - a. **SSH** to your EC2 instance and create a directory for the files to reside in, `/opt/eaglei/install`.

```
skc-macbook:~ sophia$ ssh -i "aws-eaglei-ami.pem" root@ec2-52-207-177-113.compute-1.amazonaws.com
Last login: Wed Aug 10 13:19:32 2016 from 134.174.140.154
[root@ip-172-31-54-208 ~]# mkdir /opt/eaglei/install
```

- b. In another terminal window, go to the directory containing the certificate files

- `cd /my-home/aws/cert`

- c. Do a **SCP** of the files to the newly created install folder on your EC2 instance (substitute your own file names and public hostname)

- `scp -i "aws-eaglei-ami.pem" key.pem cert.crt ca.crt root@ec2-52-207-177-113.compute-1.amazonaws.com:/opt/eaglei/install/.`

```
cd /my-home/aws/cert
scp -i "aws-eaglei-ami.pem" key.pem cert.crt ca.crt root@ec2-52-207-177-113.compute-1.amazonaws.com:/opt/eaglei/install/.
```

2. Using PuTTY/PSCP
  - a. Follow the instructions in the section *Transferring files with PSCP* at the end of the [AWS/PuTTY guide](#)

## 2. Install certificate on EC2 instance

In the **SSH** terminal,

1. Go to the install directory created above
  - `cd /opt/eaglei/install`
2. Install the certificates
  - `sh /bin/cert-install.sh -b ca.crt -c cert.crt -k key.pem`
3. At the prompt, enter the key's password. Tomcat will restart when the `cert-install.sh` script is finished.

## 3. Verify certificate has been installed correctly

Using an online **SSL validation** service, such as [http://www.geocerts.com/ssl\\_checker](http://www.geocerts.com/ssl_checker), enter your public hostname to verify that the certificate has been installed correctly

## 4. Secure cleanup

Be sure to remove the security sensitive files used for installation

```
[root@ip-172-31-54-208 install]# rm ca.crt cert.crt key.pem
```