1. **Setup a self signed certificate**

$mkdir -p docker\_reg\_certs$openssl req -newkey rsa:4096 -nodes -sha256 -keyout docker\_reg\_certs/domain.key -x509 -days 365 -out docker\_reg\_certs/domain.crt

First command will create a directory named ‘docker\_reg\_certs’ where the certificates will be saved, -p option makes the command throw error message if the folder already exists.

Second command will generate two files: **domain.key** and **domain.crt** located in docker\_reg\_certs directory.

Let’s install the certificates both in the server and the client by running these commands:

$mkdir -p /etc/docker/certs.d/ip\_address:5000$cp docker\_reg\_certs/domain.crt /etc/docker/certs.d/ip\_address:5000/ca.crt$cp docker\_reg\_certs/domain.crt /usr/local/share/ca-certificates/ca.crt$update-ca-certificates

2. **Add user authentication for registry access**

**Use htpasswd to create username and associated password**:

$mkdir docker\_reg\_auth$docker run -it --entrypoint htpasswd -v $PWD/docker\_reg\_auth:/auth -w /auth registry:2 -Bbc /auth/htpasswd admin password

**Restart docker service**:

$service docker restart

**Start registry service with the new config**:

$docker run -d -p 5000:5000 --restart=always --name registry -v $PWD/docker\_reg\_certs:/certs -v $PWD/docker\_reg\_auth:/auth -v /reg:/var/lib/registry -e REGISTRY\_HTTP\_TLS\_CERTIFICATE=/certs/domain.crt -e REGISTRY\_HTTP\_TLS\_KEY=/certs/domain.key -e "REGISTRY\_AUTH\_HTPASSWD\_REALM=Registry Realm" -e REGISTRY\_AUTH\_HTPASSWD\_PATH=/auth/htpasswd -e REGISTRY\_AUTH=htpasswd registry:2

**Verify login, push, pull and logout functionalities:**

$docker login -uadmin -ppassword ip\_address:5000

$docker push ip\_address:5000/image:tag

$docker pull ip\_address:5000/image:tag

$docker logout

To retrieve list of all repositories in your private docker registry:

$curl -u admin:password -v -X GET [https://ip\_address:5000/v2/\_catalog](https://mifos.arca-infra.com:5000/v2/_catalog)