Installing Custom CA Certificates on IoT FND

By default the FND container comes bundled with **cgms_keystore** in two locations.

- Keystore Location in the FND Container: `/opt/cgms/server/cgms/conf/`
- Keystore Location in the Linux Host: `/opt/fnd/data/`
- Keystore Name: **cgms_keystore**
- Default Password: Public123!
- Default Trusted Certification Entry in Keystore: **cisco_sudi, jmarconi**

To use a custom CA certificate on the router, add a CA certificate to the trusted certificate entries in the `cgms_keystore`:

Step 1 Place the certificate file in the following location on the host machine.

```
/opt/fnd/data/
```

Step 2 Enter into FND container.

```
docker exec -i -t fnd-container /bin/bash
```

Step 3 Change into the conf directory.

```
cd /opt/cgms/server/cgms/conf/
```

Step 4 Import a root or intermediate CA certificate to cgms_keystore.

```
/opt/cgms/jre/bin/keytool -import -trustcacerts -alias alias-name -file
/tmp/fnd-data/ca.crt -keystore cgms_keystore
```

Use a preferred alias name.

Step 5 Restart FND.

```
/etc/init.d/cgms restart
```

Step 6 Verify that the certificate was added to the trusted entry.

```
/opt/cgms/jre/bin/keytool -list -v -keystore cgms_keystore
```

Step 7 Enter keystore password.