Firebase Roles are stored as Custom Claims in the User Details. The claims Object will have the following structure:

```
{
  ‘company’: {company_name},
   ‘role’: {role_name}
}
```

{company_name}: Name of the Company user belongs to.

{role}: Role the user has in that specific company.

Following are the roles and their permissions:

1. Super Admins (super_admin)

 Has access to everything. Their company name can be null – not needed

2. Admins (admin)

 Admin of a Company has access to everything related to the company.

3.IoT Devices (iot_device)

 Has write (create, update) access to realtime_data and historical_data documents for a specific company in the Firebase. IoT Devices will use these accounts to write historical and realtime data to the Firebase.

4. Manager (manager):

 Has read and write access to all resources related to IoT Devices.

5. Monitor (monitor):

 Has read access to all IoT Device resources.