

## CREATE NEW EMPLOYEE USER – THIS IS AS A SUPER USER ADMINISTRATOR.

### 1) Initialize EMPLOYEE User Authentication

- From myAPIProject directory:  
    > python3 manage.py createsuperuser
- Username: <Enter Username:>
- Email Address: <Not Required:>
- Password: <Enter Password:>
- Confirm Password: <Re-enter Password:>

```
(venv) harrisonchen@NightNinja myApiProject % python3 manage.py createsuperuser
Username (leave blank to use 'harrisonchen'):
Email address:
Password:
Password (again):
Superuser created successfully.
(venv) harrisonchen@NightNinja myApiProject %
```

### 2) Create Authentication Token (POST Request)

- Create new POST request to: “<http://localhost:8000/api/v1/api-token-auth/> username=<Username> password=<Password>”
- Send request. If properly authenticated, response will contain authentication token.
- Alternatively in Postman:
- Create new POST request to: “<http://localhost:8000/api/v1/api-token-auth/> username=<Username> password=<Password>”
  - In Body of request, enter as Key-Value pairs:
    - username: <username>
    - password: <password>
    - Send request. If properly authenticated, response will contain authentication token for ADMINISTRATOR access.

### 3) Add Authentication Token in Subsequent Application Requests

- In ‘Headers’ tab in Postman request, enter token as:

Key: “Authorization”

Value: “Token <Authentication Token Number>”

## HOW TO CREATE NEW CUSTOMER USER – THIS IS A “NORMAL” CUSTOMER USER.

### 4) Add New CUSTOMER User Group Authentication as an Administrator.

- From Django web administrator view:
  - Go to: <http://127.0.0.1:8000/admin/auth/group/>
- Create new user by clicking “Add User” under the “Users” tab
- Add the pre-defined “CUSTOMER” permissions to your newly created user (e.g., view cart, view product, etc.)
- Save your user.
- Follow instructions below to receive Postman CUSTOMER authentication token. This token will allow CUSTOMER permissions, but will restrict ADMINISTRATOR privileges like viewing SUPPLIER and INVENTORY.

The screenshot shows the Django administration interface for a user named 'customer1'. The left sidebar has a 'Users' tab highlighted. The main content area is titled 'Change user'. The 'Username' field is set to 'customer1'. The 'Password' field shows the algorithm: pbkdf2\_sha256 iterations: 216000 salt: Hmth8M\*\*\*\*\* hash: 6LwvrB\*\*\*\*\*. The 'Permissions' section has checkboxes for 'Active', 'Staff status', and 'Superuser status'. The 'Groups' section shows 'Available groups' and 'Chosen groups', with 'Customer' selected in the 'Chosen groups' list.

### 5) Create Authentication Token (POST Request)

- In Postman:
- Create new POST request to: <http://localhost:8000/api/v1/api-token-auth/>  
username=<Username> password=<Password>” where Username and Password are the Customer username and password.
  - In Body of request, enter as Key-Value pairs:

- username: <username>
- password: <password>
- Send request. If properly authenticated, response will contain authentication token.

The screenshot shows the Postman interface for a POST request to `http://localhost:8000/api/v1/api-token-auth/`. The request body is set to `form-data` with the following fields:

KEY	VALUE	DESCRIPTION
username	ishanTest	
password	hockeysticks100	
Key	Value	Description

The response is shown in the `Body` tab, displaying a JSON object with a `token` field:

```

1 {
2   "token": "be669ec559a846138d6b94b02e78c52a9644b0ef"
3 }

```

At the top of the interface, a list of requests is visible: `POST API-auth-token`, `GET Customers - Auth...`, `POST Customers`, `GET Carts`, and three `POST http://localhost...` requests.

## 6) Add Authentication Token in Subsequent Application Requests

- In ‘Headers’ tab in Postman request, enter token as:

Key: “Authorization”

Value: “Token <Authentication Token Number>”