

Authentication

Log in

To log in:

```
POST /login
```

Parameters

- *username*: username
- *password*: password

Response

```
Status: 200 OK

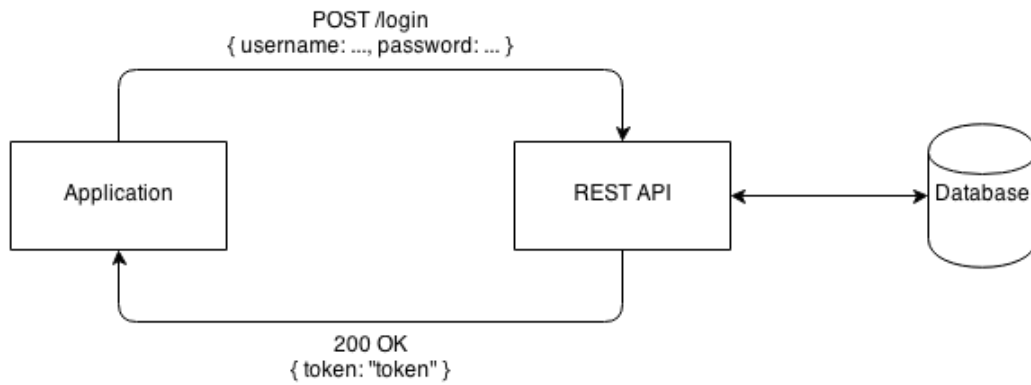
{
  "user": {
    "id": 1,
    "email": "john@doe.com",
    "name": {
      "first": "John",
      "last": "Doe"
    }
  },
  "token": "secretToken",
  "roles": []
}
```

Where:

- *user*: object representation of the user
- *token*: the web token that needs to be included with every subsequent REST API call to authenticate the request

- *roles*: array of roles that the user owns

Diagram



Log out

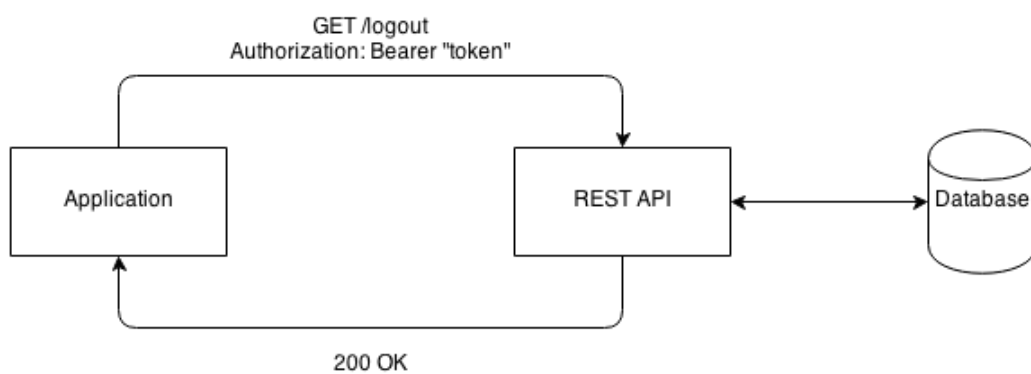
To log out:

```
GET /logout
```

Response

```
Status: 200 OK
```

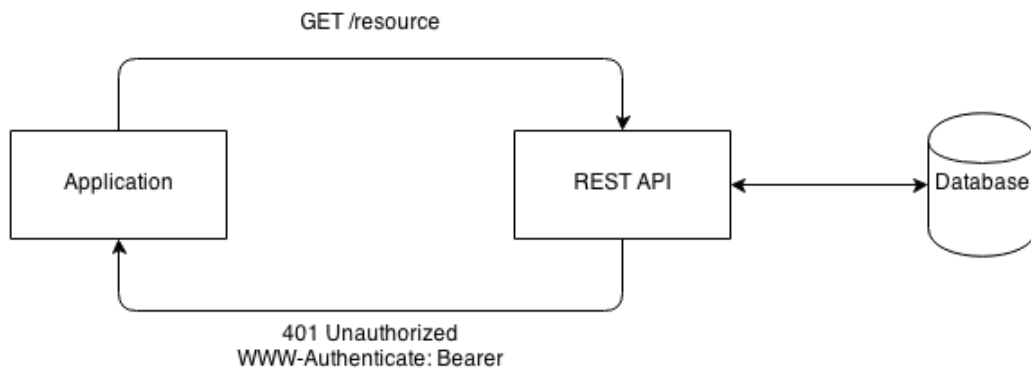
Diagram



Unauthorized requests

Unauthorized requests should be rejected by returning a `401 Unauthorized` response.

Diagram



Authorized requests

Authorized requests should send the bearer token along with the request.

Diagram

