Role-Based Access Control API Reference

Overview

The Role-Based Access Control (RBAC) API allows you to manage users, roles, and permissions within your application.

Authentication

All endpoints require a valid API token in the `Authorization` header.

```
Authorization: Bearer <token>
```

Endpoints

GET /api/v1/users

Retrieve a list of users.

Parameter	Type	Description
limit	integer	Maximum users to return.
offset	integer	Pagination offset.

```
GET /api/v1/users?limit=10&offset=0
```

POST /api/v1/users

Create a new user.

Body Parameter	Type	Description
username	string	Name of the user.
email	string	Email address.
password	string	User password.

```
POST /api/v1/users
{
  "username": "janedoe",
  "email": "jane@example.com",
  "password": "********"
}
```

GET /api/v1/roles

Retrieve a list of roles.

```
GET /api/v1/roles
```

POST /api/v1/roles

Create a new role.

Body Parameter	Type	Description
name	string	Name of the role.
permissions	array	List of permission IDs.

```
POST /api/v1/roles
{
  "name": "editor",
  "permissions": [1, 2, 3]
}
```

GET /api/v1/permissions

List all available permissions.

```
GET /api/v1/permissions
```

PUT /api/v1/users/:id/roles

Assign roles to a user.

Parameter	Type	Description
id	path	User ID.
roles	array	List of role IDs.

```
PUT /api/v1/users/8/roles
{
  "roles": [2, 4]
}
```

DELETE /api/v1/users/:id

Delete a user by ID.

```
DELETE /api/v1/users/8
```

Status Codes

- `200 OK` â€“ Success
- `201 Created` â€“ Resource created
- `400 Bad Request` â€“ Invalid input
- `401 Unauthorized` â€“ Invalid or missing token
- `404 Not Found` â€“ Resource does not exist
- `500 Internal Server Error` â€“ Server error