refresh

Overview

This API is used to refresh an expired accessToken. The user provides an unexpired refreshToken.The system will validate this refreshToken. If valid, the system will:

1. Generate a NEW accessToken and a NEW refreshToken (Refresh Token Rotation strategy).
2. Delete the OLD refreshToken that was used from the database.
3. Delete the OLD accessToken (if provided, or the user's most recent unexpired accessToken).
4. Return the new token pair to the user.

If the refreshToken is expired or invalid, the user will be forced to log in again (return a 401 error).

API Specification

API	URL
POST	/api/auth/refresh
Permission	N/A

Request sample

```
{
```

```
  "refreshToken": "aBcDeFgHiJkLmNoPQrStUvWxYz...",
  "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ..."
}
```


Field	Description	Data Type	Examples
refreshToken	Required. The user's valid refresh token.	string	aBcDeFgHi...
accessToken	Optional. Old AccessToken. If provided, this token will be deleted. Otherwise, the user's most recent token will be deleted.	string	eyJhbGci...

Response sample


```
{
  "statusCode": 200,
  "message": "Tokens refreshed successfully",
  "data": {
    "accessToken": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ... (NEW)",
    "refreshToken": "zYxWvUtSrQpOnMlKjIhGfEdCbA... (NEW)"
  },
  "responsedAt": "2023-10-28T10:40:00.789Z"
}
```


Validation

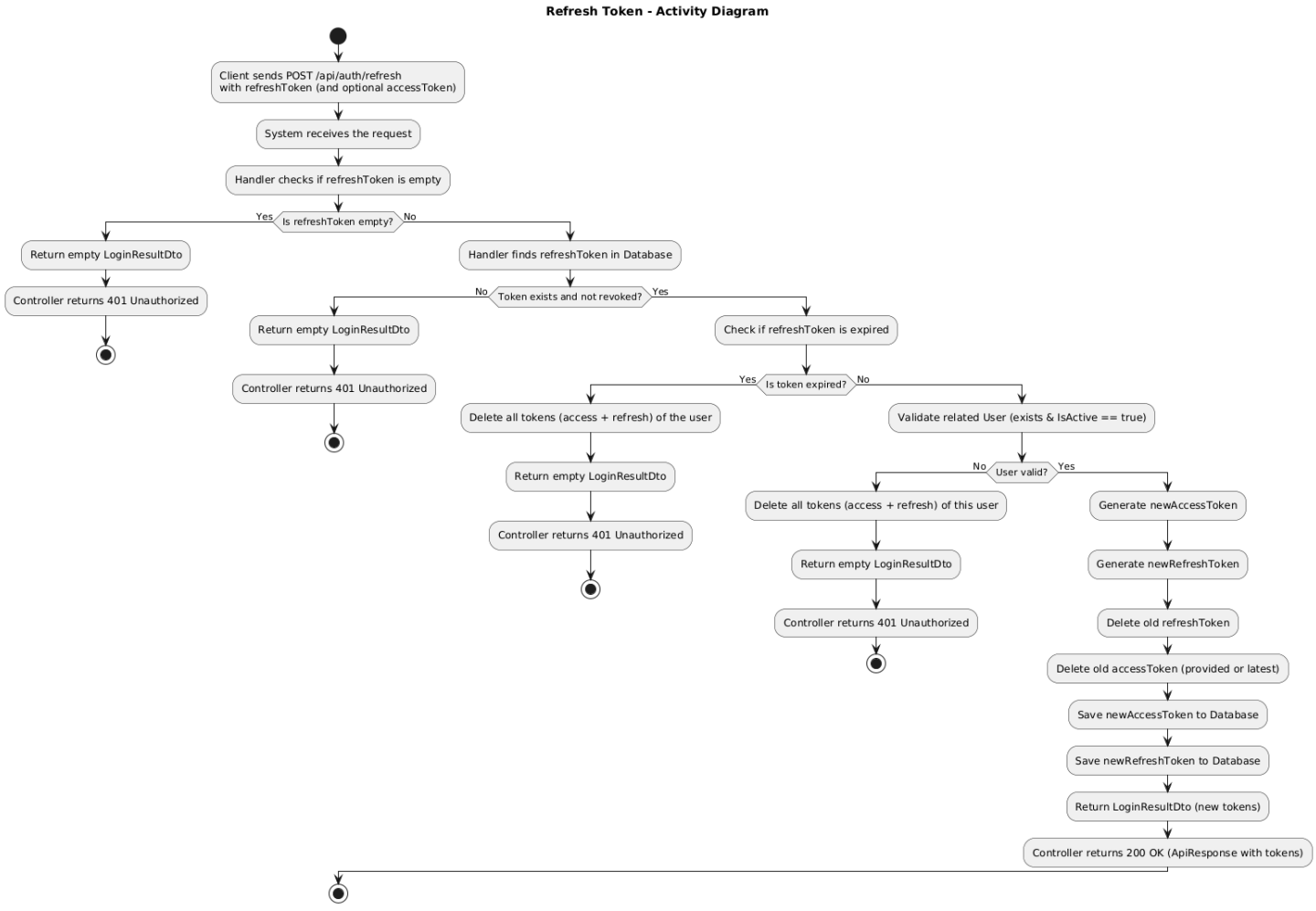
Status code	Description	Examples

401	refreshToken is missing in request.	{ "statusCode": 401, "message": "Invalid or expired refresh token. Please login again.", "data": null, "responsedAt": "..." }
401	refreshToken not found in database.	{ "statusCode": 401, "message": "Invalid or expired refresh token. Please login again.", "data": null, "responsedAt": "..." }

401	refreshToken has been revoked (IsRevoked = true).	{ "statusCode": 401, "message": "Invalid or expired refresh token. Please login again.", "data": null, "responsedAt": "..." }
401	refreshToken has expired (ExpiresAt < DateTime.UtcNow).	{ "statusCode": 401, "message": "Invalid or expired refresh token. Please login again.", "data": null, "responsedAt": "..." }

401	refreshToken is valid but the associated user does not exist or has been disabled (IsActive = false).	{ "statusCode": 401, "message": "Invalid or expired refresh token. Please login again.", "data": null, "responsedAt": "..." }

Activity Diagram



Sequence Diagram