Login Endpoint - English

Description

This endpoint authenticates users by validating an Auth0 access token and an email encoded in Base64. If the authentication is successful, it generates a JWT for the user's session and a URL that will allow the user to be redirected to the application.

URL

POST `/api/login`

Authentication

Required Token: Auth0 access token

- **Obtaining the Token**: You must register your application with Auth0 and configure it to use the authorization flow that best suits your needs (e.g., Client Credentials, Authorization Code, etc.). The access token should be requested from Auth0 using the `client_id`, `client_secret`, and appropriate scopes that allow access to this endpoint.
- **Using the Token**: The access token must be included in all requests to the login endpoint in the authorization header as a Bearer Token.

Headers

Key	Value	Description
Authorization	`Bearer {token}`	Auth0 access token required for authentication.

Body Parameters

Parameter	Required	Type	Description

`email`	Yes	string	The user's email encoded in Base64 format.
`redirect_url`	No	string	URL to which the user will be redirected if the callback token is expired or invalid.

Request Example

```
curl -X POST "https://yourdomain.com/api/login" \
-H "Authorization: Bearer {auth0_access_token}" \
-H "Content-Type: application/json" \
-d '{"email": "dXNlckBleGFtcGxlLmNvbQ==", "redirect_url": "https://yourdomain.com/login"}'
```

Success Response

Code: 200 OK

```
{
  "status": "success",
  "url": "https://yourdomain.com/site/callback?token=jwt_token_here&redirect_url=url_to_redirect",
  "token": "jwt_token_here",
  "expires_in": 1718082360,
  "message": "User logged in"
}
```

Description: The response includes the status of the operation, a descriptive message, and a URL with the generated JWT and the redirect URL in case of an error as a parameter.

Error Responses

- **401 Unauthorized** (with `redirect_url` provided):

If the Auth0 token is invalid or has expired, and a `redirect_url` is provided, the user is redirected to that URL.

- **400 Bad Request** (Email missing):

```
{
  "status": "error",
  "message": "Email is required"
```

```
}
```

Response Data

Field	Type	Description
`status`	string	The status of the response, can be "success" or "error".
`url`	string	URL to which the client may be redirected, includes the JWT in successful responses and the redirect URL in case the callback generates an error.
`token`	string	The JWT generated for the user session.
`expires_in`	int	Token expiration time in seconds.
`message`	string	Descriptive message about the outcome of the operation.

Possible Error Values

Code	Message	Description
401	Unauthorized or invalid token	Indicates that the provided Auth0 token is invalid or expired. If `redirect_url` is provided, the user is redirected.
400	Email is required	Email was not provided in the request body.
400	Username invalid	The username does not exist in the system.
400	User doesn't have any licence	The user lacks the necessary licensing.
400	User doesn't have a profile	The user does not have an associated profile.
400	Unknown error	An unspecified error occurred.

This documentation now accurately reflects the behavior of the endpoint when dealing with expired or invalid Auth0 tokens, including the redirection to a specified URL if provided. This ensures a clear and comprehensive understanding for all potential users and developers interacting with the API.

Revision #5
Created 6 May 2024 10:15:53 by Danny Rios Tolosa
Updated 2 September 2024 08:29:06 by Danny Rios Tolosa