API Palace

- Login Endpoint - Español
- Login Endpoint - English

Login Endpoint - Español

Descripción

Este endpoint autentica a los usuarios validando un token de acceso de Auth0 y un correo electrónico codificado en Base64. Si la autenticación es exitosa, genera un JWT para la sesión del usuario y una URL que permitira al usuario ser redirigido a la aplicación.

URL

`POST /api/login`

Autenticación

Token Requerido: Access token de Auth0

- **Obtener el Token**: Debes registrar tu aplicación con Auth0 y configurarla para utilizar el flujo de autorización que mejor se adapte a tus necesidades (por ejemplo, Client Credentials, Authorization Code, etc.). El token de acceso debe solicitarse a Auth0 utilizando el `client_id`, `client_secret` y los scopes adecuados que permitan acceder a este endpoint.
- **Uso del Token**: El token de acceso debe ser incluido en todas las solicitudes al endpoint de login en el header de autorización como un Bearer Token.

Headers

Key	Value	Description
Authorization	Bearer {token}	Token de acceso de Auth0 necesario para la autenticación.

Parámetros del cuerpo (Body)

Parámetro	Requerido	Tipo	Descripción
email	Sí	String	Correo electrónico del usuario codificado en base64.

Parámetro	Requerido	Tipo	Descripción
redirect_url	Sí	String	URL a la que se redirigirá al usuario si el token del callback está vencido o es inválido.

Ejemplo de Petición

```
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"}'
```

Respuestas

Success Response

Código: 200 OK

Contenido del cuerpo:

```
{
  "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"
}
```

Descripción: La respuesta incluye el estado de la operación, un mensaje descriptivo, y una URL con el JWT generado y la url de redirección en caso de error como parámetro.

Error Responses

Código: 401 Unauthorized

Contenido del cuerpo:

```
{
  "status": "error",
  "message": "Unauthorized or invalid token"
```

```
}
```

Descripción: Se retorna cuando el token de Auth0 no es válido o ha expirado.

Código: 400 Bad Request

Contenido del cuerpo:

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

Descripción: Se retorna cuando no se ha incluido el correo electrónico en la solicitud.

Datos de Respuesta

Campo	Tipo	Descripción
status	string	Estado de la respuesta, puede ser "success" o "error".
url	string	URL a la que el cliente puede ser redirigido, incluye el JWT en respuestas exitosas y la url de redireccion en caso que el callback genere error
token	string	El JWT generado para la sesión del usuario.
expires_in	int	Tiempo de expiración del token en segundos.
message	string	Mensaje descriptivo sobre el resultado de la operación.

Tabla de Posibles Valores de Error en Message

Código	Mensaje	Descripción
401	Unauthorized or invalid token	Indica que el token de Auth0 proporcionado es inválido o está vencido.
400	Email is required	No se proporcionó un correo electrónico en el cuerpo de la solicitud.
400	Username invalid	El nombre de usuario no existe en el sistema.
400	User doesn't have any licence	El usuario no tiene la licencia necesaria.
400	User doesn't have a profile	El usuario no tiene un perfil asociado.
400	Unknown error	Ocurrió un error no especificado.

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.

Parameter	Required	Type	Description
`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.