Access Tokens - Auth0 Docs

Archived: 2026-04-05 17:03:27 UTC

are used in token-based authentication to allow an application to access an API. The application receives an access token after a user successfully authenticates and authorizes access, then passes the access token as a credential when it calls the target API. The passed token informs the API that the bearer of the token has been authorized to access the API and perform specific actions specified by the that was granted during authorization. In addition, if you have chosen to allow users to log in through an , such as Facebook, the will issue its own access token to allow your application to call the IDP's API. For example, if your user authenticates using Facebook, the access token issued by Facebook can be used to call the Facebook Graph API. These tokens are controlled by the IdP and can be issued in any format. See Identity Provider Access Tokens for details.

Opaque access tokens

Opaque access tokens are tokens in a proprietary format that you cannot access and typically contain some identifier to information in a server's persistent storage. To validate an opaque token, the recipient of the token needs to call the server that issued the token. In Auth0's case, opaque tokens can be used with the `/userinfo` endpoint to return a user's profile. If you receive an opaque Access Token, you don't need to validate it. You can use it with the `/userinfo` endpoint, and Auth0 takes care of the rest. To learn more, see Get Access Tokens.

(JWT) access tokens conform to the JWT standard and contain information about an entity in the form of claims. They are self-contained therefore it is not necessary for the recipient to call a server to validate the token. Access tokens issued for the and access tokens issued for any custom API that you have registered with Auth0 follow the JWT standard, which means that their basic structure conforms to the typical JWT structure, and they contain standard JWT claims asserted about the token itself.

Management API access tokens

An access token issued for the Auth0 Management API should be treated as opaque (regardless of whether it actually is), so you don't need to validate it. You can use it with the Auth0 Management API, and Auth0 takes care of the rest. To learn more, see Auth0 Management API Tokens.

Custom API access tokens

If validation of your custom API access token fails, make sure it was issued with your custom API as the `audience`. To learn more, see Get Access Tokens.

Sample access token

This example shows the contents of an access token. Notice that the token only contains authorization information about the actions the application is allowed to perform at the API (such permissions are referred to as `scopes`).

```
{
 "iss": "https://my-domain.auth0.com/",
 "sub": "auth0|123456",
 "aud": [
   "https://example.com/health-api",
   "https://my-domain.auth0.com/userinfo"
 ],
 "azp": "my_client_id",
 "exp": 1311281970,
 "iat": 1311280970,
 "scope": "openid profile read:patients read:admin"
}
```

The token does not contain any information about the user except for the user ID (located in the `sub` claim). In many cases, you may find it useful to retrieve additional user information. You can do this by calling the userinfo API endpoint with the Access Token. Be sure that the API for which the Access Token is issued uses the **RS256** signing algorithm.

Access token security

You should follow token best practices when using access tokens, and for JWTs, make sure that you validate an access token before assuming that its contents can be trusted.

Access token lifetime

Custom API token lifetime

By default, an access token for a custom API is valid for 86400 seconds (24 hours). We recommend that you set the validity period of your token based on the security requirements of your API. For example, an access token that accesses a banking API should expire more quickly than one that accesses a to-do API. To learn more, see Update Access Token Lifetime.

/userinfo endpoint token lifetime

Access tokens issued strictly for the purpose of accessing the OIDC `/userinfo` endpoint have a default lifetime and can't be changed. The length of lifetime depends on the flow used to obtain the token:

Flow	Lifetime
Implicit	7200 seconds (2 hours)
Authorization Code/Hybrid	86400 seconds (24 hours)

Learn more

- Get Access Tokens
- Validate Access Tokens
- Use Access Tokens
- Token Best Practices
