Web Endpoint

Generate and validate tokens

Validate an authorization grant code delivered to your app to obtain tokens, or validate an existing refresh token.

AccountOrganizationalDataSharing 1.0+

URL

```
POST https://appleid.apple.com/auth/oauth2/v2/token
```

HTTP Body

`form-data` The list of input parameters required for the server to validate the authorization code or refresh token.
Content-Type: application/x-www-form-urlencoded

Parts

`client_id`
`string`
(Required) The identifier (App ID or Services ID) for your app. To help prevent the possibility of exposing sensitive data to the end user, the identifier must not include your Team ID.

`client_secret`
`string`
(Required) A secret JWT, generated by the developer, that uses the Account and Organizational Data Sharing private key associated with your developer account. Authorization code and refresh token validation requests require this parameter.

`code`
`string`
The authorization code received in an authorization response sent to your app. The code is single-use only and valid for five minutes. Authorization code validation requests require this parameter.

grant_type
string

(Required) The grant type determines how the client app interacts with the validation server. Authorization code and refresh token validation requests require this parameter. For authorization code validation, use `authorization_code`. For refresh token validation requests, use `refresh_token`.

redirect_uri
string

The destination URI provided in the authorization request when authorizing a user with your app, if applicable. The URI must use the HTTPS protocol, include a domain name, and can't contain an IP address or `localhost`. Authorization code requests require this parameter.

refresh_token
string

The refresh token received from the validation server during an authorization request. Refresh token validation requests require this parameter.

Response Codes

200
TokenResponse

OK
The request was successful.
Content-Type: application/json

400
ErrorResponse

Bad Request
The server was unable to process the request.
Content-Type: application/json

Overview

The validation server returns a `TokenResponse` object in the response body of a successful validation request. Use this endpoint to either authorize a user by validating the authorization code received by your app, or by validating an existing refresh token to verify a user session or obtain access tokens.

Validate the authorization grant code

When you send an authorization request to the validation server, include the following form data parameters:

- `client_id`
- `client_secret`
- `code`
- `grant_type`
- `redirect_uri`

> **Note**
>
> When authorizing a user with your app, include the `redirect_uri` parameter only if the application provided a `redirect_uri` in the initial authorization request.

For information on how to create the JWT that you use as the client secret, see Creating a client secret.

The following is an example authorization validation request URL via `curl`:

```
curl -v POST "https://appleid.apple.com/auth/oauth2/v2/token" \
-H 'content-type: application/x-www-form-urlencoded' \
-d 'client_id=CLIENT_ID' \
-d 'client_secret=CLIENT_SECRET' \
-d 'code=CODE' \
-d 'grant_type=authorization_code' \
-d 'redirect_uri=REDIRECT_URI'
```

After the server validates the authorization code, the endpoint returns the identity token, an access token, and a refresh token. The following is an example authorization validation response:

```
{
    "access_token": "adg61...670r9",
    "token_type": "Bearer",
    "expires_in": 3600,
    "refresh_token": "rca7...lABoQ",
    "id_token": "eyJra...96sZg"
}
```

Use the refresh token to verify the user session from the server and obtain access tokens.

Validate an existing refresh token

When performing a validation request, you must include the following form data parameters:

- `client_id`
- `client_secret`
- `grant_type`
- `refresh_token`

For information on how to create the JWT you use as the client secret, see Creating a client secret.

The following is an example validation request URL using `curl`:

```
curl -v POST "https://appleid.apple.com/auth/oauth2/v2/token" \
-H 'content-type: application/x-www-form-urlencoded' \
-d 'client_id=CLIENT_ID' \
-d 'client_secret=CLIENT_SECRET' \
-d 'grant_type=refresh_token' \
-d 'refresh_token=REFRESH_TOKEN'
```

After the server validates the refresh token, the endpoint returns the identity token and an access token. The following is an example refresh token validation response:

```
{
  "access_token": "beg510...670r9",
  "token_type": "Bearer",
  "expires_in": 3600,
  "id_token": "eyJra...96sZg"
}
```

See Also

Generating tokens

Creating a client secret

Generate a signed token to identify your client application.

`Fetch Apple's public key for verifying token signature`

Retrieve the public key associated with the cryptographic identity Apple uses to sign the token.