Web Endpoint

Revoke tokens

Invalidate the tokens and associated user authorizations for someone when they are no longer associated with your app.

AccountOrganizationalDataSharing 1.0+

URL

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

HTTP Body

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

Parts

`client_id`
`string`
(Required) The identifier (App ID or Services ID) for your app. The identifier must match the value provided during the authorization request for the person's information. To help mitigate the possibility of exposing sensitive data to the end user, the identifier must not include your Team ID.
Content-Type: text/plain

`client_secret`
`string`
(Required) A secret JWT that uses the Account and Organizational Data Sharing private key associated with your developer account. For more information about creating client secrets, see `Generate and validate tokens`.
Content-Type: text/plain

`token`
`string`
(Required) The user refresh token or access token intended to be revoked. If the request is successful, revoke the user session associated with the provided token.
Content-Type: text/plain

token_type_hint string	A hint about the type of the token submitted for revocation. Use `refresh_token` or `access_token`. Content-Type: text/plain

Response Codes

200	**OK** The request was successful; the provided token has been revoked successfully or was previously invalid. Content-Type: application/json
400 ErrorResponse	**Bad Request** The server was unable to process the request. See the error code description for more information about the underlying error. Content-Type: application/json

Overview

To revoke authorization for a user, you must obtain a valid refresh token or access token. If you don't have either token for the user, you can generate tokens when validating an authorization code. For more information about user tokens and creating client secrets, see Generate and validate tokens.

To invalidate a user's refresh token, invoke the revoke endpoint with the following HTTP POST method:

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

Additionally, to invalidate a user's access token, use the following HTTP POST method:

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

For either token revocation request, the revoke endpoint returns a `200` response code without a response body after the server invalidates the `token` value, or if the token was previously invalidated. If the server encounters an error, it returns an `ErrorResponse` that identifies the problem.

See Also

Using and revoking tokens

`Request an authorization`

Request a user authorization to Account & Organizational Data Sharing apps and web services.