Google Cloud

Edge Security

OAuth Introduction

Proprietary + Confidential

OAuth overview

OAuth v2.0

is a protocol that allows clients to grant access to server resources to another entity without sharing credentials

Client IDs and Secrets

are used to identify and authenticate applications (application's consumer key and consumer secret)

Tokens

are issued to allow access to specific resources for a specified period of time and may be revoked by the user that granted permission or by the server that issued the token

Scopes

can be used to limit the access for a given token, granting permission only for the operations that are necessary

Grant Types

4 different Grant Types specify the different authentication usage scenarios OAuth supports

TLS

Tokens must be protected, and OAuth 2.0 requires that all API traffic be sent via TLS

Access tokens

Access Tokens allow access to a protected resource for a specific application to perform only certain actions for a limited period of time.

In Edge, access tokens are opaque strings with no encoded meaning. Access tokens are passed as Bearer tokens in an Authorization header.

Identification info from the requesting application (client ID and secret)

+

Resource owner credentials (optional: user of the app)

+

Optional information about what the application wants to do with the resource (scope)

=

Access Token and (optional) refresh token

Refresh tokens

- Refresh Tokens, if provided, represent a limited right to reauthorize the granted access by obtaining new access tokens.
- In Edge, refresh tokens are opaque strings with no encoded meaning.

Identification info from the requesting application (client ID and secret)

+

Refresh token

+

Optional information about what the application wants to do with the resource (scope)

=

Access Token

Scopes

Scopes identify what an application can do with the resources it is requesting access to.

Scope names are defined by the authorization server and are associated with information that enables decisions on whether a given API request is allowed or not.

When an application requests an access token, the scope names are optional

Edge associates scope names to be matched with a combination of API resource path and verb. So, for example:

Scope 1: "READ"

- GET /photos
- GET /photos/{id}

Scope 2: "UPDATE"

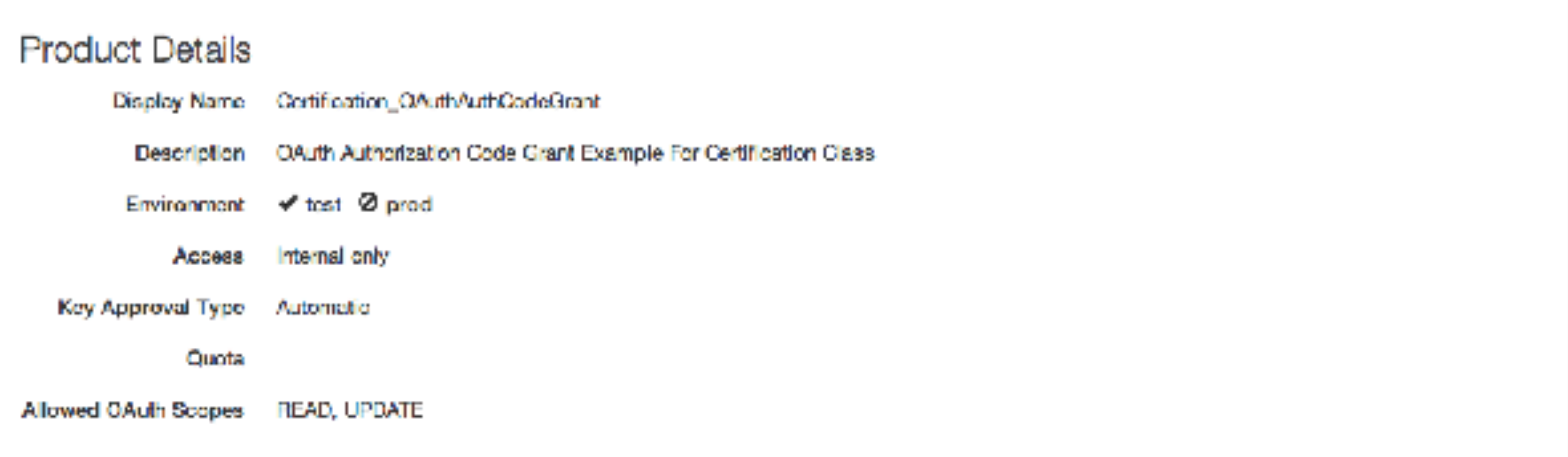
- GET /photos
- GET /photos/{id}
- POST /photos
- PUT /photos/{id}

Scopes

The OAuth spec allows for an app to specify no scope on a token request, in which case you should either:

- assign a default scope or no scopes (the usual case), or
- reject the request

One or more scopes can be specified in the API Product definition



Product Details

Display Name	Certification_OAuthAuthCodeGrant
Description	OAuth Authorization Code Grant Example For Certification Class
Environment	✓ test ⊘ prod
Access	Internal only
Key Approval Type	Automatic
Quota	
Allowed OAuth Scopes	READ, UPDATE

OAuth grants

An OAuth Grant is a credential representing the resource owner's authorization. More often than not, we tend to think of grants in terms of the process used to obtain an access token.

Grant Type	Typical Use Case	Complex?
No specific resource owner is involved		
Client Credentials	Business system interactions, where resources being operated on are owned by the partner, not a particular user	No
A specific resource owner is involved		
Resource Owner Password Credentials	Resources are owned by a particular user and the requesting application is trusted	A bit
Authorization Code	Resources are owned by a particular user and the requesting application is untrusted	Very
Implicit	Resources are owned by a particular user, and the requesting application is an untrusted browser-based app written in a scripting language such as JavaScript	Very complex, and less secure than Auth Code

THANK YOU