Laravel-Cognito-OAuth APIs

Overview

Version information

Version : 1.0.0

Contact information

Contact : Crea7dosSantos
Contact Email : crea7dos3tos@gmail.com

Tags

- OAuth : 認証に関する取り扱いを行います

Paths

認可エンドポイント

```
GET /oauth/authorize
```

Description

認可エンドポイントは、認証サーバーによって提供されるエンドポイントで、HTTPS GETのみをサポートします。

リライング・パーティは通常、このリクエストをブラウザ経由で行います。

PKCEを使用した認可エンドポイントへのリクエスト例

https://localhost/oauth/authorize?client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&
response_type=code&state=STATE&code_challenge=CODE_CHALLENGE&
code_challenge_method=S256

Parameters

Type	Name	Description	Schema
Query	**client_id** *required*	クライアントIDです。 認証サーバーに対して、事前登録したリライング・パーティのクライアントIDを指定する必要があります。必須のパラメータです。	string
Query	**code_challenge** *optional*	PKCEでを使った認可コードグラントで利用されるパラメータの一つで、code_verifierに対してcode_challenge_methodの計算をほどこして算出された値です。 code_verifierはRFC7376仕様（https://datatracker.ietf.org/doc/html/rfc7636）で定義されているように、文字、数字、記号文字を含む43文字から128文字のランダムな文字列でなければなりません。code_verifierに対してcode_challenge_methodのハッシュ値を計算し、それにBase64URLエンコードを施したものがcode_challengeになります。任意のパラメータです。	string
Query	**code_challenge_method** *optional*	PKCEでを使った認可コードグラントで利用されるパラメータの一つで、code_challenge_methodの値は「S256」を利用してください。 「plain」を指定すると、code_challengeが流出した場合、全く同じ値であるcode_verifierも流出したことになります。任意のパラメータです。	string
Query	**redirect_uri** *required*	リダイレクトURIはリライング・パティーのURIです。 リダイレクトURIは認証サーバーが発行した認可コードの受け渡し先になります。認証が行われると、認証サーバーはステータスコード302のレスポンスを返してブラウザをリダイレクトURIにリダイレクトします。その際、クエリパラメータの形で認可コードが渡されます。 認証サーバーに対してリライング・パーティを事前登録する際に、指定したURIをパラメータとして指定する必要があります。必須のパラメータです。	string
Query	**response_type** *required*	レスポンスのタイプです。 安全にアクセストークン（JWT）やリフレッシュトークンを認証サーバーで生成する為に、「code」を指定してください。必須のパラメータです。	string

Type	Name	Description	Schema
Query	**state** *optional*	ランダムな文字列です。 認証サーバーはリライング・パーティを登録する際に指定した、リダイレクトURIにリダイレクトレスポンスを返す際に、この値を含めます。リライング・パーティはトークンエンドポイントに認可コードを用いてリクエストする前に、stateパラメータを検証することで、CSRFを防ぐために利用することができます。任意のパラメータです。	string

Responses

HTTP Code	Description	Schema
302	HyperText Transfer Protocol (HTTP) の 302 Found リダイレクトステータスレスポンスコードは、リクエストされたリソースが一時的にLocationで示されたURLへ移動したことを示します。 **Headers** : `Location` (string) : ログイン画面へのURLが含まれます。（例: http://localhost/login）.	No Content

Tags

- OAuth

トークンエンドポイント

```
POST /oauth/token
```

Description

トークンエンドポイントは、認証サーバーによって提供されるエンドポイントで、HTTPS　POSTのみをサポートします。

リライング・パーティはブラウザ経由でなく、このエンドポイントに直接リクエストを送信します。

PKCEを使用したトークンエンドポイントへのリクエスト例（認可コードを使用したトークンのリクエスト）

https://localhost/oauth/token?grant_type=authorization_code&client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&code_verifier=CODE_VERIFIER&code=CODE

PKCEを使用したトークンエンドポイントへのリクエスト例（更新トークンを使用したトークンのリフレッシュ）

https://localhost/oauth/token?grant_type=refresh_token&client_id=CLIENT_ID&redirect_uri=REDIRECT_URI&refresh_token=REFRESH_TOKEN

Parameters

Type	Name	Description	Schema
Query	**client_id** *required*	クライアントIDです。 認証サーバーに対して、事前登録したリライング・パーティのクライアントIDを指定する必要があります。必須のパラメータです。	string
Query	**code** *optional*	リダイレクトレスポンスに付与された認可コードです。 認可コードは「grant_type」 に「authorization_code」を指定した際に必須のパラメータになります。	string
Query	**code_verifier** *optional*	PKCEでを使った認可コードグラントで利用されるパラメータの一つで、リライング・パーティが認可エンドポイントにリクエストを送信する前に生成した値です。 認証サーバーはリライング・パーティから送信されたこの値を、認可エンドポイントのリクエストに含められたcode_challenge とcode_challenge_methodから検証し、一致する場合は、トークンをレスポンスとして返します。	string
Query	**grant_type** *required*	トークン付与タイプです。 「authorization_code」か「refresh_token」を指定してください。「authorization_code」が指定された場合に、認証サーバーはこの値を持って、認可コードグランによるトークンリクエストであることを知ります。 「refresh_token」という値を指定する際は、トークンを更新する際に利用します。必須のパラメータです。	string

Type	Name	Description	Schema
Query	**redirect_uri** *optional*	リダイレクトURIはリライング・パティーのURIです。 リダイレクトURIは認証サーバーが発行した認可コードの受け渡し先になります。認可エンドポイントでクエリパラメータとして含めた値を指定します。 認証サーバーに対してリライング・パーティを事前登録する際に、指定したURIをパラメータとして指定する必要があります。「grant_type」に「grant_type」に「authorization_code」を指定した場合は、必須のパラメータになります。	string
Query	**refresh_token** *optional*	リフレッシュトークンです。 「grant_type」に「refresh_token」を指定した場合は、必須のパラメータになります。	string

Responses

HTTP Code	Description	Schema
200	認証サーバーからリクエスト成功時に返却されるレスポンスです。	Tokens
401	認証サーバーからリクエスト失敗時に返却されるレスポンスです。	UnAuthorizedError
500	認証サーバーで処理できない場合に返却されるレスポンスです。	InternalServerError

Tags

- OAuth

Definitions

InternalServerError

サーバー側で処理方法がわからない事態が発生したことを示します。

Name	Description	Schema
message *optional*	**Example** : "エラーが発生しました。再度時間を空けてお試しください"	string

Tokens

認証サーバーから返却されるトークンです。

Name	Description	Schema
access_token *optional*	このパラメーターの値として入っている文字列がアクセストークンです。アクセストークンはクライアントからリソースサーバーに対するアクセスに利用されます。クライアントからリソースサーバーに対するすべてのアクセスに、アクセストークンが含まれていなければなりません。 **Example** : `"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJhdWQiOiI5Njk0N2FhMy05MGJjLTRiMzAtYWE2Mi0wNmY5YjE2YmM0NWMiLCJqdGkiOiI5NzFkOWM3NGIwNDQzODg0OWMxMTJhYTRkM2VlZjVlMTlmZGFmZjQxOGJhMTY1MjFiM2ViNTNhNTk0Njk2YmZmN2IzMmM4ZTM1YjEzN2E5MCIsImlhdCI6MTY1NjMwMDM3Ny44ODI5MjQsIm5iZiI6MTY1NjMwMDM3Ny44ODI5MywiZXhwIjoxNjU2MzAyMTc3Ljg0Nzg2NCwic3ViIjoiMSIsInNjb3BlcyI6W119.mb9aLTgTstXrQJlnfVPPRVY-R9IUOzuTTO5B65DCOixuzP5MUcMTYU89p2AATdJcyjLJcvKW5pKPwyN29NsgxaR7cwywbJTx5-PHRLmrbFOLYlUPcMf20IAGfeyII-mow2KcSo2kfwsuMx2FoppBwEhu51yCG0nyimTuoPpQrJ_paeJE8xgODXztX_SW2tgf9kaAnX_jj0DU0Si4b6ReUPkq-hfjs_iAMerRjLfsMf6kpFAo2agh8EWcSHDCOOeY9vL0pJLVNEwKcqlOOJYjrka9igknYWfbUf_RFDvQNzjzP021pgMod_suSk_RGN4RpC_XbzivWw8BgYLUnaKelPjFbPf1OJvADOmpIybS2nTCp19l-wadLvYbdF7LYnHa9kfi77Rn0dIfoVJaOIkokstTyn7FtSdut9KcLkZToj-iOU1-ylHHn46vqbRSL-A4EELyVAqPtLwzR3YzlHijyxDMTrXS51eSqS8EcaK0gkwds9_2gg9ycuKfgkBzX9SThFvhe43Rdyo7H197zM_5boNbPr9mHOqTzQtHKyzqTCFtEMf97kzfnYd64RGIF2S1T4UbYSt1DEWQEB9dD-HJJib0ObOT_csnWZWcEnDRVMMKlQq_RbKOi-VthecevgudBs7FNOacU8_1m-dTfQRKwXScxv_WS7OJL3f0_fiA_4"`	string
expires_in *optional*	アクセストークンの有効期限が秒単位で入っています。例えば、この値が3600　の場合、有効期限は1時間であることを示しています。 **Example** : `"1800"`	string

Name	Description	Schema
refresh_token *optional*	このパラメーターとして入っている文字列がリフレッシュトークンです。リフレッシュトークンは、クライアントから認可サーバーに対してアクセストークンの 再発行を要求する際に利用されます。 **Example** : "def5020022b1aa52cf1a5ddae5e2c0dd0fc13cc462f46aee348db91713b897039c29ed9411f7c335604b9f2ff80595e0b0e11257c243c42987ebda8f40118972403e3d6550d12d116d7986638f052d3a154d604635999ee3dabda470c941f5ea2eb8a491a4ce48ac108542382128f0c193fcb7add70f43c300cb66308b5f62b3bfb105893ccd5a2a5511b384123754157f2576fc3e1239d663a7b822bb11f51a46a23808ac2d388381b359e42db2222668a9c030d2f0967015501b5bc583ce37d9411dc42484360d697d64aebee423d5b78cbac4533b154e8919cc62479a9774537b73be7165390b29f507539007920d2a41a5e90a92cac073acf9115cb3158f45d56c06266c7bd3b543211551a1d8eed960c5a9d1faffb618293622dbe8371abac1aeca47e7820c0a660eec9e197be062adb672b87a189763cf13f56ac40d1f12c34d414b47f84a4f8ed862fec32e9447b9dc03ec2bb3194d697e05716af19d77c2a4cb3dd2fe067599e83f75876724c26f76d75c9db8b66693f6fc9fe10416e6182b62"	string
token_type *optional*	Bearerという値が入っています。Bearerトークンであることを示しています。 **Example** : "Bearer"	string

UnAuthorizedError

HTTP標準ではunauthorized(不許可)と定義されていますが、意味的にはこのレスポンスはunauthenticated(未認証)です。つまり、クライアントはリクエストされたレスポンスを得るためには認証を受けなければなりません。

Name	Description	Schema
message *optional*	**Example** : "アクセストークンの有効期限が切れています"	string