

Il s'agit d'une description du flux OAuth2 provenant de sites Web tiers.

Dans le flux d'application Web (également appelé flux de code d'autorisation), le propriétaire de la ressource (un utilisateur 42) est d'abord redirigé par l'application vers le serveur d'autorisation OAuth du fournisseur d'API. Le serveur d'autorisation vérifie si l'utilisateur a une session active (dans notre cas, si l'utilisateur est connecté à l'intranet 42). Si c'est le cas, le serveur d'autorisation lui demande d'accéder aux données demandées. Une fois l'accès accordé, il est redirigé vers l'application Web et un code d'autorisation est inclus dans l'URL en tant que paramètre de requête de

code : `http://www.example.com/oauth_callback?code=ABC1234`

Étant donné que le code est transmis en tant que paramètre de requête, le navigateur Web l'envoie au serveur Web qui agit en tant que client OAuth. Ce code d'autorisation est ensuite échangé contre un jeton d'accès à l'aide d'un appel de serveur à serveur de l'application au serveur d'autorisation. Ce jeton d'accès est utilisé par le client pour effectuer des appels d'API.

Voyons comment nous pouvons l'implémenter avec l'API 42.

Rediriger les utilisateurs pour demander l'accès 42

C'est la première étape. Liez ou redirigez les utilisateurs vers l'URL d'autorisation de l'API :

`https://api.intra.42.fr/oauth/authorize` . Celle-ci doit être correctement formatée pour votre application et renverra un écran d'autorisations pour que l'utilisateur puisse l'autoriser. Pour plus de commodité, une URL d'autorisation formatée incluant votre `client_id` est fournie pour chaque application dans la page des applications (`https://profile.intra.42.fr/oauth/applications`) .

URL de base

```
GET https://api.intra.42.fr/oauth/authorize
```

Paramètres

Nom	Type	Description
<code>client_id</code>	chaîne	Obligatoire . L'identifiant client que vous avez reçu de 42 lors de votre inscription (<code>https://profile.intra.42.fr/oauth/applications/new</code>) .
<code>redirection_uri</code>	chaîne	Obligatoire . L'URL de votre application vers laquelle les utilisateurs seront redirigés après autorisation. Voir les détails ci-dessous sur les URL de redirection .


Nom	Taper	Description
portée	chaîne	Liste de portées séparées par des espaces. Si elle n'est pas fournie, <code>scope</code> la valeur par défaut est une liste de portées vide pour les utilisateurs qui ne disposent pas d'un jeton valide pour l'application. Pour les utilisateurs qui disposent déjà d'un jeton valide pour l'application, la page d'autorisation OAuth avec la liste des portées ne s'affiche pas. Au lieu de cela, cette étape du flux se termine automatiquement avec les mêmes portées que celles utilisées la dernière fois que l'utilisateur a terminé le flux.
État	chaîne	Une chaîne aléatoire impossible à deviner. Elle est utilisée pour se protéger contre les attaques de falsification de requêtes intersites.
type_de_réponse	chaîne	Le type de réponse. Habituellement <code>code</code> .

Tous ces éléments constitueront ensemble une URI agréable et compréhensible, comme :

```
https://api.intra.42.fr/oauth/authorize?client_id=your_very_long_client_id&redirect_uri=http%3A%2F%2Flocalhost%3A1919%2Fusers%2Fauth%2Fft%2Fcallback&response_type=code&scope=public&state=a_very_long_random_string_witchmust_be_unguessable'
```

Petite remarque : lors du formatage des paramètres de portée, assurez-vous de lire ci-dessus la distinction entre les portées au niveau de l'application et au niveau du jeton. Cela a été un point de friction pour certains développeurs.

42 redirections vers votre site

 dialogue_d'authentification La boîte de dialogue d'authentification 42

Si l'utilisateur accorde l'autorisation à votre application d'utiliser les données demandées (voir les portées), elle sera redirigée vers votre `redirect_uri` avec un code temporaire dans un `code` paramètre GET ainsi que l'état que vous avez fourni à l'étape précédente dans un `state` paramètre.

Si les états ne correspondent pas, la demande a été créée par un tiers et le processus doit être interrompu.

Échangez votre code contre un jeton d'accès

Vous y êtes presque ! La dernière chose à faire est une requête POST vers le

`https://api.intra.42.fr/oauth/token` point de terminaison, avec votre `client_id`, votre `client_secret`, le précédent `code` et votre `redirect_uri`. **Cette requête doit être effectuée côté serveur, via une connexion sécurisée.**

Note inutile : ceci correspond au point de terminaison du jeton, section 3.2 de la RFC OAuth 2. Heureux ?

URL de base

```
POST https://api.intra.42.fr/oauth/token
```

Paramètres

Nom	Taper	Description
type_de_subvention	chaîne	Obligatoire . Le type de subvention. Dans ce cas, il s'agit <code>authorization_code</code> de.
client_id	chaîne	Obligatoire . L'identifiant client que vous avez reçu de 42 lors de votre inscription.
client_secret	chaîne	Obligatoire . Le secret client que vous avez reçu de 42 lors de votre inscription.
code	chaîne	Obligatoire . Le code que vous avez reçu en réponse à l'étape 1.
redirection_uri	chaîne	L'URL de votre application où les utilisateurs seront envoyés après autorisation.
État	chaîne	La chaîne aléatoire non devinable que vous avez éventuellement fournie à l'étape 1.

Par exemple, avec curl :

```
curl -F grant_type=authorization_code \
-F client_id=9b36d8c0db59eff5038aea7a417d73e69aea75b41aac771816d2ef1b3109cc2f \
-F client_secret=d6ea27703957b69939b8104ed4524595e210cd2e79af587744a7eb6e58f5b3d2 \
-F code=fd0847dbb559752d932dd3c1ac34ff98d27b11fe2fea5a864f44740cd7919ad0 \
-F redirect_uri=https://myawesomeweb.site/callback (https://myawesomeweb.site/callback) \
-X POST https://api.intra.42.fr/oauth/token (https://api.intra.42.fr/oauth/token)
```

Frapper

Effectuez des requêtes API avec votre token

Incluez votre jeton dans toutes vos demandes dans un en-tête d'autorisation :

```
Authorization: Bearer YOUR_ACCESS_TOKEN
```

Par exemple, vous pouvez récupérer le propriétaire actuel du jeton, avec curl :

```
curl -H "Authorization: Bearer YOUR_ACCESS_TOKEN" https://api.intra.42.fr/v2/me (https # {"id":56911,"email":"pedago@staff.42.fr (mailto:id)","login":"30_1","url":"http://lo
```

Frappier

Si vous ne pouvez pas modifier les en-têtes http, vous pouvez envoyer votre jeton en `access_token` paramètre.

Spécification (/apidoc/guides/specification)

Commencer (/apidoc/guides/getting_started)

Flux d'application Web (/apidoc/guides/web_application_flow)

Rediriger les utilisateurs pour demander l'accès 42

42 redirections vers votre site

Échangez votre code contre un jeton d'accès

Effectuez des requêtes API avec votre token

Contribuer (/apidoc/guides/contributing)

Lisez-moi (/apidoc/guides/README)

Fièrement fabriqué avec des tonnes de  par l'unité de développement.