Authorization Without User Consent

All APIs require authorization, but for certain APIs, user consent is not necessary. A request for authorization without consent uses OAuth 2.0 with a grant type of **client_credentials**. You will need the app key and secret that was created by the Developer Program website.

URL:

```
POST https://api.att.com/oauth/token
```

Request headers:

Header Name	Required	Description
Accept	Optional	The format of the data that should be returned. Valid values are **application/json** and **application/xml.** Default is **application/json**.
Content-Type	Required	The format of the data that is in the POST body. Must be set to **application/x-www-form-urlencoded**.

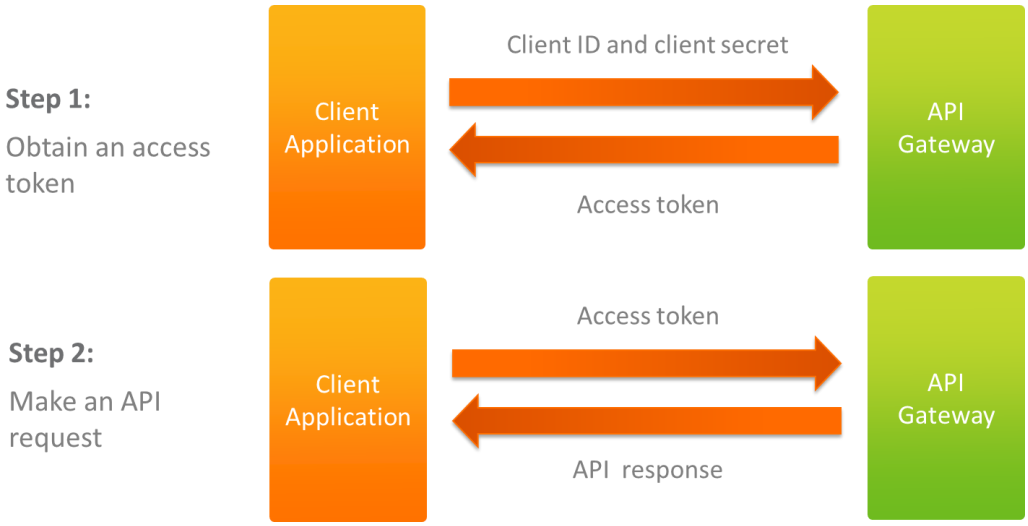
The POST body contains key/value pairs with these parameters:

Parameter	Required	Description
grant_type	Required	Set to **client_credentials**.
client_id	Required	Your app's app key.
client_secret	Required	Your app's secret.
scope	Required	Which API requests will be used with this token. Use a comma-delimited list if you are requesting more than one.

The response has these elements:

Element Name	Description
access_token	The token to be used in making other API requests.
token_type	The type of token to returned. Typically "bearer".
expires_in	The expiration time, in seconds. A value of **0** means that it never expires.
refresh_token	The token to be used when the access token expires, in order to retrieve a new access token.

Authorization flow:



Authorization Without User Consent: Example

Sample Request

```
POST https://api.att.com/oauth/token
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Content-Length: 119

client_id=ABCDEF0123456789ABCDEF0123456789&
    client_secret=ABCDEF0123456789&
    grant_type=client_credentials&
    scope=SMS,MMS,SPEECH,STTC,TTS
```

URL

The format to be returned: application/json or application/xml.

The format of the data in the POST body: application/x-www-form-urlencoded.

POST body

The app key.

The app secret.

The grant type is client_credentials

The APIs you want to use

Note: Carriage returns added for improved readability. Requests must be url-form-encoded with no white space.

Sample Response

```
{
  "access_token":"4a0e9c2b14a0548addb29eb77e06a8b",
  "token_type":"bearer",
  "expires_in":"157679999",
  "refresh_token":"f40caf9ef81261882752186087f600
}
```

Token to use in API requests

The type of token returned

Expiration time in seconds

Token to use if your access token expires

Authorization With Consent

If you are reading or writing user-sensitive data, such as a device's location or capabilities, then you need authorization with consent. This type of request uses OAuth 2.0 with a grant type of **authorization_code**. You will need the app key and secret that was created by the Developer Program website.

URL to obtain an authorization code:

```
https://api.att.com/oauth/authorize?client_id={appkey}&scope={scope}
```

→ *where* `{appkey}` *is the app key and* `{scope}` *is a comma-delimited list of APIs to authorize.*

URL that is navigated to once consent is obtained:

```
http://{redirect-url}?code={code}
```

→ *where {redirect-url} is specified in the app details on the developer portal, and {code} is the authorization code.*

URL to obtain access token:

```
POST https://api.att.com/oauth/token
```

Request headers:

Header Name	Required	Description
Accept	Optional	The format of the data that should be returned. Valid values are **application/json** and **application/xml**. Default is **application/json**.
Content-Type	Required	The format of the data that is in the POST body. Must be set to **application/x-www-form-urlencoded**.

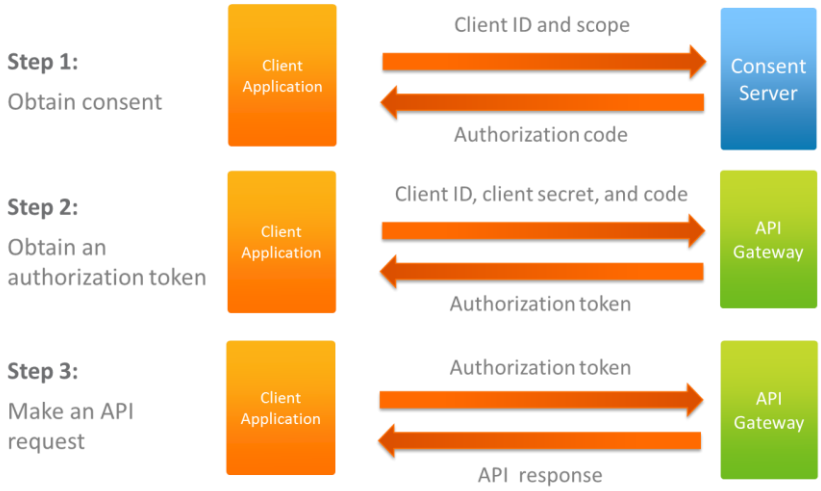
The POST body contains key/value pairs with these parameters:

Parameter	Required	Description
grant_type	Required	Set to **authorization_code**.
client_id	Required	Your app's app key.
client_secret	Required	Your app's secret.
code	Required	The authorization code that was returned with the redirected URL.

The response has these elements:

Element Name	Description
access_token	The token to be used in making other API requests.
token_type	The type of token to returned. Typically "bearer".
expires_in	The expiration time, in seconds. A value of **0** means that it never expires.
refresh_token	The token to be used when the access token expires, in order to retrieve a new access token.

Authorization flow



Authorization With Consent: Example

Sample Request to Put in Browser

```
https://api.att.com/oauth/authorize?
  client_id=822d66045a3a89852d4b9&scope=IMMN
```

App key

Which APIs to use

Sample URL that Is Returned After Consent

```
http://redirect.example.com/index.html?
  code=243gZiyL9bTiUrRDRTMhwb
```

Authorization code

Sample Request

```
POST https://api.att.com/oauth/token
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Content-Length: 119

client_id=ABCDEF0123456789ABCDEF0123456789&
    client_secret=ABCDEF0123456789&
    code=ABCDEF0123456789ABCDEF&
    grant_type=authorization_code
```

URL

The format to be returned: application/json or application/xml

The format of the data in the POST body: application/x-www-form-urlencoded

The app key.

The app secret.

The code returned after obtaining consent

The grant type is authorization_code

Note: Carriage returns added for improved readability. Requests must be url-form-encoded with no white space.

Sample Response

```
{
  "access_token":"4a0e9c2b14a0548addb29eb77e06a8b",
  "token_type":"bearer",
  "expires_in":"157679999",
  "refresh_token":"f40caf9ef8126188275218(
}
```

Token to use in API requests

The type of token returned

Expiration time in seconds

Token to use if your access token expires

Using the Refresh Token

If your authorization token is about to expire, you can use the refresh token to obtain a new one. The refresh token is returned with every request to the **token** resource.

URL:

```
POST https://api.att.com/oauth/token
```

Request headers:

Header Name	Required	Description
Accept	Optional	The format of the data that should be returned. Valid values are **application/json** and **application/xml**. Default is **application/json**.
Content-Type	Required	The format of the data that is in the POST body. Must be set to application/x-www-form-urlencoded.

The POST body contains key/value pairs with these parameters:

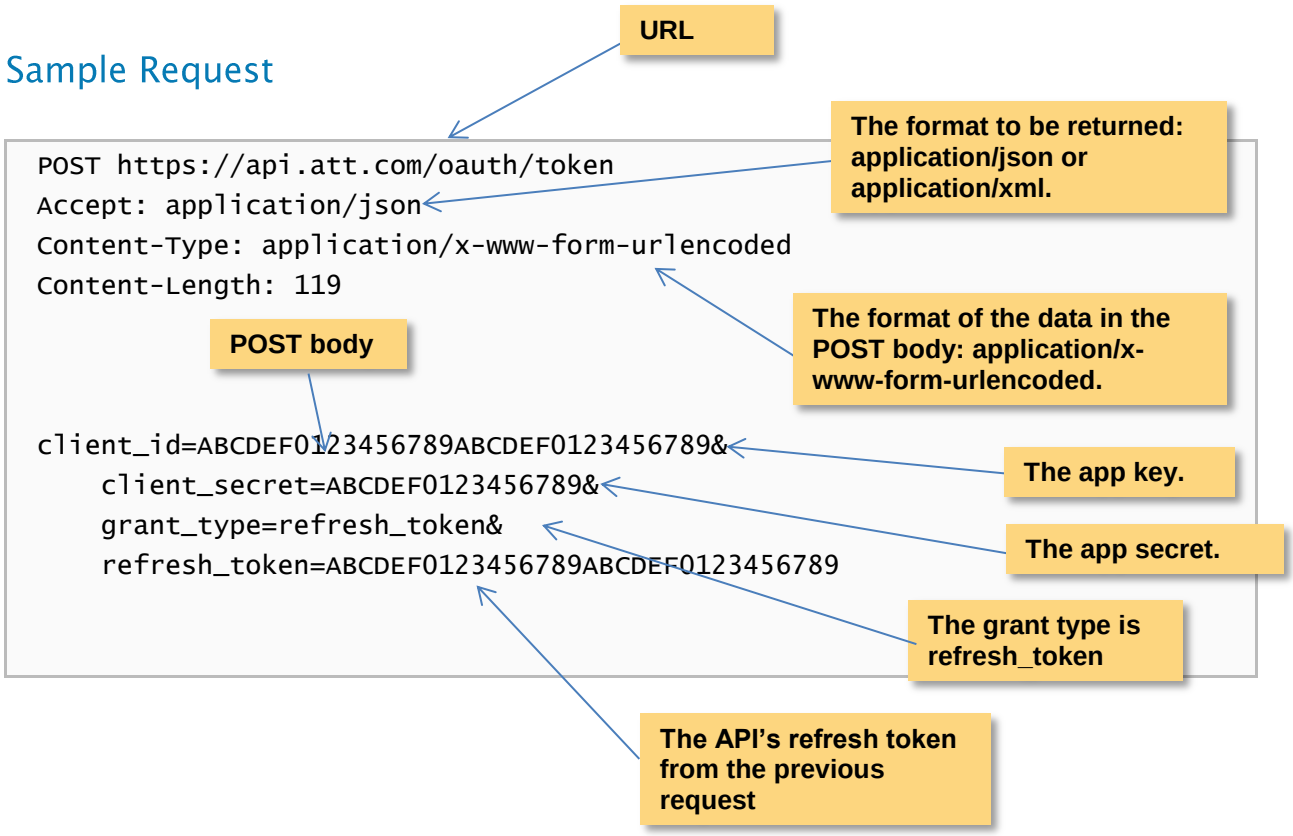
Parameter	Required	Description
grant_type	Required	Set to **refresh_token**.
client_id	Required	Your app's app key.
client_secret	Required	Your app's secret.
refresh_token	Required	The refresh token from your previous call to receive an access token.

The response has these elements:

Element Name	Description
access_token	The token to be used in making other API requests.
token_type	The type of token to returned. Typically "bearer".
expires_in	The expiration time, in seconds. A value of **0** means that it never expires.
refresh_token	The refresh token.

Using the Refresh Token: Example

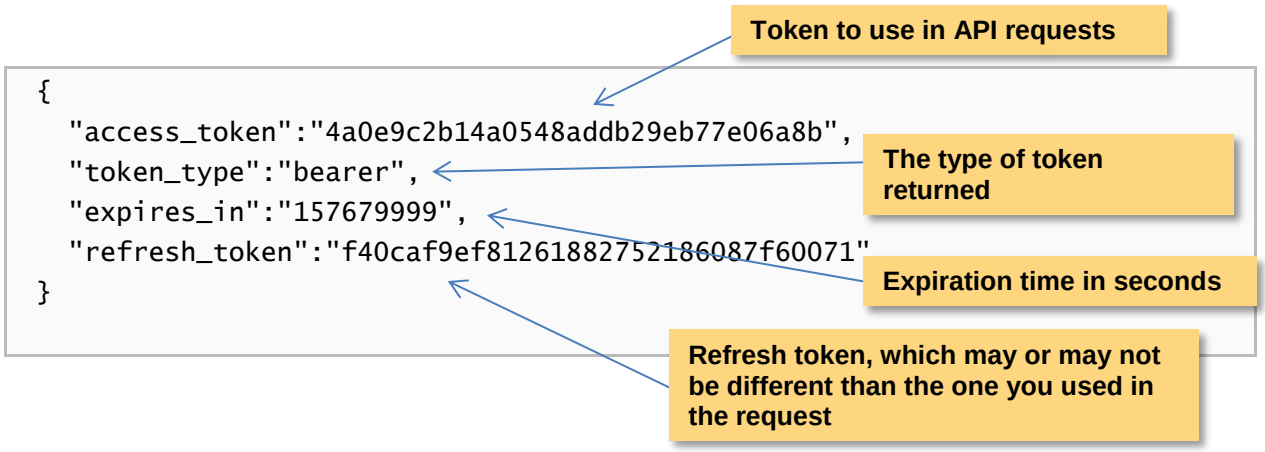
Sample Request




```
POST https://api.att.com/oauth/token
Accept: application/json
Content-Type: application/x-www-form-urlencoded
Content-Length: 119

client_id=ABCDEF0123456789ABCDEF0123456789&
    client_secret=ABCDEF0123456789&
    grant_type=refresh_token&
    refresh_token=ABCDEF0123456789ABCDEF0123456789
```

Sample Response




```
{
  "access_token":"4a0e9c2b14a0548addb29eb77e06a8b",
  "token_type":"bearer",
  "expires_in":"157679999",
  "refresh_token":"f40caf9ef81261882752186087f60071"
}
```