





6.

6.  "application/x-www-form-urlencoded"  HTTP  UTF-8 

- grant_type
 "refresh_token" 
- refresh_token
- scope 



3.2.1

 HTTP 

```
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JWContent-Type: application/x-www-form-urlencoded
grant_type=refresh_token&refresh_token=tGzv3J0kF0XG5Qx2TlKWIA
```


3.19.2



6. Refreshing an Access Token

If the authorization server issued a refresh token to the client, the client makes a refresh request to the token endpoint by adding the following parameters using the "application/x-www-form-urlencoded" format per Appendix B with a character encoding of UTF-8 in the HTTP

request entity-body:

grant_type

REQUIRED. Value MUST be set to "refresh_token".

refresh_token

REQUIRED. The refresh token issued to the client.

scope

OPTIONAL. The scope of the access request as described by Section 3.3. The requested scope MUST NOT include any scope not originally granted by the resource owner, and if omitted is treated as equal to the scope originally granted by the resource owner.

Because refresh tokens are typically long-lasting credentials used to request additional access tokens, the refresh token is bound to the client to which it was issued. If the client type is confidential or

the client was issued client credentials (or assigned other authentication requirements), the client MUST authenticate with the

authorization server as described in Section 3.2.1.

For example, the client makes the following HTTP request using transport-layer security (with extra line breaks for display purposes

only):

POST /token HTTP/1.1

Host: server.example.com

Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token&refresh_token=tGzv3J0kF0XG5Qx2TlKWIA

Hardt

Standards Track

[Page 47]

RFC 6749

OAuth 2.0

October 2012

The authorization server MUST:

- o require client authentication for confidential clients or for any client that was issued client credentials (or with other authentication requirements),

- o authenticate the client if client authentication is included and ensure that the refresh token was issued to the authenticated client, and

- o validate the refresh token.

If valid and authorized, the authorization server issues an access token as described in

Section 5.1. If the request failed verification or is invalid, the authorization server returns an error

response as described in Section 5.2.

The authorization server MAY issue a new refresh token, in which case the client MUST discard the old refresh token and replace it with the new refresh token. The authorization server MAY revoke the old refresh token after issuing a new refresh token to the client. If a

new refresh token is issued, the refresh token scope MUST be identical to that of the refresh token included by the client in the request.

Revision #1

Created Wed, Mar 25, 2020 11:07 PM by []

Updated Wed, Mar 25, 2020 11:07 PM by []