

Refresh Token and Consent Expiration

IETF 123 (Jul 25, 2025) 

Nick Watson (Google LLC)

Recap: refresh token expiration

Two related but different concepts:

- Consent expiration: how long is the user's consent good for (e.g. user opts for 30-day consent)
- Credential expiration: how long is the returned credential good for (e.g. when implementing RT rotation)

Recap: refresh token expiration

- For consent expiration, clients wish to remind the user of upcoming consent expiration while the user is active to avoid interruption of service if consent expires while the user is inactive.
- For RT rotation, clients need to know how often an RT must be used.

I-D Links

<https://datatracker.ietf.org/doc/draft-watson-oauth-refresh-token-expiration/>

<https://github.com/njwatson32/rt-expiration>

draft-watson-oauth-refresh-token-expiration

00
Jun 2025

Spec tl;dr

Two new token endpoint response params.

`refresh_token_expires_in`

The lifetime in seconds of the refresh token. This value SHALL NOT exceed the value in `consent_expires_in`.

`consent_expires_in`

The lifetime in seconds of the user's consent. This value MAY exceed that of `refresh_token_expires_in`.

Questions for Group

- Use case for defining parameter(s) for clients to request time-limited tokens?
 - Authorization flow request
 - Token endpoint request
- Worth adding any non-normative implementation notes about how consent expiration may be set/selected?
- Any reviewers? :)