OAuth 2.0
Incremental Auth

IETF 101 London, March 2018

William Denniss

Recap: Incremental Auth
Problem Statement

Asking for the kitchen sink of scopes up-front is a bad thing.

Users should have the context of the authorization request.

E.g. Granting a calendar scope only makes sense in the context of interacting with a calendar-related feature.
Hi Bill

billd1600@gmail.com

Google OAuth 2.0 Playground wants to

- View and manage the files in your Google Drive
- Manage your Blogger account
- Send email on your behalf
- Manage your contacts
- Manage your calendars
- Manage your YouTube account

Allow Google OAuth 2.0 Playground to do this?

By clicking Allow, you allow this app to use your information in accordance to their terms of service and privacy policies. You can remove this or any other app connected to your account in My Account.
Incremental Auth Definition

The ability to request additional scopes in subsequent requests resulting in a single authorization grant representing all scopes granted so far.
Typical Implementation

Consent screen should only display new scopes (or display new/existing scopes differently).

Single refresh token issued for the union of all granted scopes.
De-facto Incremental Auth for Confidential Clients

OAuth 2.0 doesn’t stop you returning an authorization grant with *more* scope, so many people have implemented this already for confidential clients.
Public Client Protocol “Appcremental”

New token endpoint param: `existing_grant`.

When exchanging the authorization code from subsequent (i.e. incremental) requests, pass the previous refresh token in `existing_grant`.

Resulting access and refresh tokens will contain a union of the scope.
Incremental Auth for Native Apps

App → Authorization Endpoint

Initial Authorization Request

Authorization Request (Scope A)

Response: authorization_code

Token Request: authorization_code

Response: access_token, refresh_token

App

Authorization Endpoint

Incremental Authorization Request

Authorization Request (Scope B)

Response: authorization_code (Scope B)

Token Request: authorization_code (Scope B), existing_grant (Scope A)

Response: access_token, refresh_token (Scope A, B)

Token Endpoint
Combined Grant $A \cup B$
Google’s OAuth server already supports incremental auth for public clients, as defined in this spec.

Try out my proof of concept:
https://github.com/WilliamDenniss/AppAuth-iOS/tree/appcremental
Demo

https://youtu.be/SPSCW4NUooU
Confidential Client Specification Details

Documents best practices, security considerations, and:

New authorization endpoint parameter
include Granted scopes.
Updates since IETF 99

Sections added:

- Security Considerations
- Privacy Considerations
- Usability Considerations
- Alternative Approaches

OAuth 2.0 Incremental Auth

Discuss