INTERNET-DRAFT
Intended status: Informational
Expires: 13 November 2025

Francis A. Medeiros-Logeay
University of Oslo

13 May 2025

Manual OAuth 2.0 Configuration Profile for Mail Clients
draft-francis-oauth2-mail-client-manual-config-00

Abstract

This document defines a lightweight and interoperable profile for configuring OAuth 2.0 authentication in mail clients using a small number of manually entered parameters. The profile targets public clients using PKCE and discovery endpoints, avoiding the need for dynamic client registration or hardcoded provider logic. The goal is to make secure OAuth 2.0-based authentication for IMAP/SMTP universally deployable and user-configurable.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 November 2025.

Introduction

OAuth 2.0 and OpenID Connect are increasingly used for authenticating users to mail servers over IMAP and SMTP. However, mail clients today face interoperability challenges due to the lack of a standardized, manual configuration method that works across OAuth 2.0 providers.

This document defines a profile that allows mail clients to interoperate with any compliant authorization server using a simple set of manually entered configuration fields. It assumes the client is a public native application using PKCE and that the server provides a compliant discovery endpoint.

This approach avoids the complexity and limited support of dynamic client registration, while promoting secure and consistent behavior for users and developers.

Terminology

The key words "MUST", "MUST NOT", "SHOULD", and "MAY" are to be interpreted as described in RFC 2119.

Profile Overview

This profile describes how a user or client can configure an email application using the following fields:

Required Fields

Field	Description
‘discovery_url‘	URL of the OAuth 2.0 discovery endpoint, e.g., ‘https://mail.example.com/.well-known/oauth-authorization-server‘
‘client_id‘	Public client ID (e.g., ‘thunderbird‘, ‘my-mail-app‘)
‘scopes‘	Space-separated string of requested scopes (e.g., ‘openid email imap smtp‘)

Optional/Assumed

- ‘redirect_uri‘: MAY be predefined by the client (e.g., ‘urn:ietf:wg:oauth:2.0:oob‘ or a registered custom URI).
- ‘code_challenge_method‘: MUST be ‘S256‘
- ‘token_endpoint_auth_method‘: MUST be ‘none‘

User Configuration Simplification

Implementations SHOULD allow users to enter only the base domain (e.g., idp.example.com) rather than a full discovery URL. Clients MAY automatically derive the full discovery URL by appending /.well-known/oauth-authorization-server or /.well-known/openid-configuration to the base domain, as appropriate, in accordance with [RFC 8414].

Client Behavior

Clients implementing this profile MUST:

- Use [RFC 7636] PKCE with ‘S256‘.
- Use the ‘.well-known/openid-configuration‘ endpoint to retrieve ‘authorization_endpoint‘, ‘token_endpoint‘, and supported capabilities.
- Use the ‘client_id‘ provided by the user or a pre-registered one.
- Allow manual entry of the configuration fields defined in Section 4.
- Obtain authorization codes using the authorization code flow.
- Authenticate to the token endpoint without a client secret.

Server Requirements

Authorization servers supporting this profile MUST:

- Support public clients without client secrets.
- Support the [RFC 7636] PKCE extension with ‘S256‘.
- Provide a compliant discovery document at the ‘discovery_url‘.
- Support scopes necessary for mail access (e.g., ‘imap‘, ‘smtp‘, ‘email‘).
- Accept known redirect URIs or support native app mechanisms like ‘urn:ietf:wg:oauth:2.0:oob‘.

Security Considerations

This profile assumes a native client operating as a public OAuth 2.0 client. As such:

- PKCE is required to protect authorization code exchanges.
- No client secret is used or required.
- Client IDs are not confidential.

Servers MUST use secure communication (TLS) and validate redirect URIs to prevent injecti
on or phishing.

IANA Considerations

This document has no IANA actions.

References

Normative References

- [RFC6749] D. Hardt, *The OAuth 2.0 Authorization Framework*, October 2012.
- [RFC7636] N. Sakimura et al., *Proof Key for Code Exchange by OAuth Public Clients*, Se
ptember 2015.
- [RFC8414] M. Jones, *OAuth 2.0 Authorization Server Metadata*, June 2018.

Informative References

- [RFC8252] B. Campbell and W. Denniss, *OAuth 2.0 for Native Apps*, October 2017.

Acknowledgements

Thanks to the OAuth and Mailmaint working groups for their discussions and feedback.

Appendix A: Example Configuration

A mail client might allow the user to enter:

Discovery URL: https://mail.example.com/.well-known/oauth-authorization-server
Client ID: thunderbird
Scopes: openid mail

The rest of the configuration (endpoints, redirect URIs, etc.) is derived from discovery.

Author’s Address

Francis Augusto Medeiros-Logeay
University of Oslo
Email: franciaa@usit.uio.no