Web Authorization Protocol
Internet-Draft
Intended status: Standards Track
Expires: 21 May 2026

E. Smith
17 November 2025

# OAuth Authorization Management URI
## draft-emelia-oauth-authorization-management-uri-00

## Abstract

This specification defines a authorization_management_uri property for the OAuth Authorization Server Metadata ([RFC8414]), which allows an authorization server to specify a URI through which the user may manage the authorized clients that have access to their account.

## About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://drafts.thisismissem.social/draft-emelia-oauth-authorization-management-uri.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-emelia-oauth-authorization-management-uri/.

Discussion of this document takes place on the Web Authorization Protocol Working Group mailing list (mailto:oauth@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/oauth/. Subscribe at https://www.ietf.org/mailman/listinfo/oauth/.

Source for this draft and an issue tracker can be found at https://github.com/ThisIsMissEm/draft-oauth-authorization-management-uri.

## 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/.

## Copyright Notice



## Table of Contents



## 1. Introduction

An OAuth 2.0 [RFC6749] client may wish to provide access to a web-based UI at which a user can manage the applications authorized to access their account with the Authorization Server. This is a feature many Authorization Servers already support, however, when you don't have a primary service for the Authorization Server, there may be no clear path for a user to access this management page. This is especially true for decentralized social web applications where the mapping between Authorization Servers and Clients is many to many.

This specification defines the new property of authorization_management_uri for the OAuth Authorization Server Metadata, as defined in [RFC8414]. This URI should point to a website at which the user can manage the authorizations that they have granted with their Authorization Server (for example, to revoke any client or active session, or review the security history of their account).

## 2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

## 3. Authorization Management UI

An Authorization Server may provide a user interface through which users can manage the OAuth Clients that have access to their account, such that users can manage their account security with the Authorization Server. This user interface is typically at an URI specific to the Authorization Server implementation, and requires authentication to access.

This specification does not define specifics of the user interface, however, recommends that the user interface allows a user to manage their account security and authorized clients with the Authorization Server, for example, allowing them to see all authorized clients that have access to their account.

To allow OAuth Clients to discover the URI of this user interface, this specification defines the new property authorization_management_uri for the OAuth Authorization Server Metadata, as defined in [RFC8414].

## 4. Security Considerations

This specification does not define how the Authorization Server should security the authorization management UI. Authorization Servers should take appropriate measures to ensure that the user is authenticated and authorized to view the authorization management UI.

The OAuth Client MUST NOT open the authorization_management_uri in a webview or similar embedded browser, and instead delegate that to the users’ default browser, such that the OAuth Client has no access to the account credentials or to other sensitive data.

## 5. IANA Considerations

### 5.1. OAuth Authorization Server Metadata Registry

The following authorization server metadata value is defined by this specification and registered in the IANA "OAuth Authorization Server Metadata" registry established in OAuth 2.0 Authorization Server Metadata [RFC8414].

* Metadata Name: authorization_management_uri

* Metadata Description: URI of the authorization management user interface provided by the Authorization Server.

* Change Controller: IETF

* Specification Document: [draft-emelia-oauth-authorization-management-uri-00]

## 6. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/rfc/rfc6749>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8414] Jones, M., Sakimura, N., and J. Bradley, "OAuth 2.0 Authorization Server Metadata", RFC 8414, DOI 10.17487/RFC8414, June 2018, <https://www.rfc-editor.org/rfc/rfc8414>.

## Author’s Address

Emelia Smith
Email: emelia@brandedcode.com
URI: https://thisismissem.social