Upcoming Changes in FAMAuth v2.12

Target Deployment Date: (12/2/2025)

Version 005

November 21, 2025

Revision Log

Rev #	Date	Author	Description
001	5/8/25	Marshall Keppel	Initial revision
002	6/16/25	Mike Roadifer	Added OAuth changes
003	7/9/25	Mike Roadifer	Updated "Available in QA"
004	7/11/25	Mike Roadifer	Update to OAuth Breaking Changes
005	11/21/25	Mike Roadifer	Updates to OAuth Breaking Changes and OAuth New Features.

Table of Contents

USDA Forest Service
Fire and Aviation Management – Information Management

OAuth Breaking Changes
Available in QA: No

The FAMAuth back-end has been upgraded from Spring v5 to v6 which includes changes to the OAuth services that may break the OAuth2 integration for applications.

1. The /oauth/token service no longer accepts URL parameters. Systems will need to change to send the same data in the request entity-body (rfc6749#section-4.4.2).

> https://famauth.wildfire.gov/oauth/token?grant_type=authorization_code&redirect_url=https://myurl.gov&code=d5TsjY
>
> https://famauth.wildfire.gov/oauth/token&refresh_token=eulsh5k…

2. The /oauth/check_token service no longer accepts URL parameters to validate an access_token. Systems will need to change to send the same data in the request entity-body. This service now requires basic authentication to be sent containing the registered application's client_id and client_secret (rfc7662#section-2.1). This service is now able to validate the access_token, refresh_token or id_token.

3. The /me service accepts the access_token as either a URL parameter, or a Bearer token in the Authorization header, but not both.

4. The refresh token is no longer a JWT and is now considered opaque to the client.

Note that these changes adhere to RFC6749 (https://datatracker.ietf.org/doc/html/rfc6749), RFC6750 (https://datatracker.ietf.org/doc/html/rfc6750) and RFC7662 (https://datatracker.ietf.org/doc/html/rfc7662).

OAuth New Features
Available in QA: No

1. The /oauth/jwks service will return JSON web key sets to be used to validate JWT tokens (access_token or id_token) returned by the authorization server.

2. OpenID Connect (OIDC) is now supported (in addition to OAuth2). The OIDC equivalent user information service to the OAuth2 /me serivce is /userinfo. To use OIDC an application must send scope=openid on the /oauth/authorize service call.
/.well-known/openid-configuration is the new service to get the OIDC meta data.

3. Retrieving a new access_token using the refresh_token now returns the reusable refresh_token on every call and no longer requires applications to store off the first refresh_token returned for use on every call.

4. The token service now returns a claim value of "refresh_token_expires_in" which is the difference between the current time and when the refresh token will expire. Client applications can use this value to warn users when they are nearing the point of needing to re-authenticate.

Add Client ID to Manage Applications Grid
Available in QA: No

The purpose of this enhancement is to add Client ID (the primary key for the application) to the application management grid so that Application Managers can see the unique key for an application tile.

Thank you!

Please reach out to Ryan Hunt (Ryan.Hunt2@usda.gov) or Mike Roadifer (Michael.Roadifer@usda.gov) for more information.