Aras OAuth Registry 32

Release Notes

Document #: D-009187

Last Modified: *8/22/2024*

Copyright Information

Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
Phone: 978-806-9400

Notice of Rights

Notice of Liability

This document is provided for informational purposes only, and the contents hereof are subject to change without notice. The information contained in this document is distributed on an "As Is" basis, without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose or a warranty of non-infringement. Aras shall have no liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this document or by the software or hardware products described herein.

Table of Contents

Send Us Your Comments

Aras Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is important in determining the information used for future revisions.

- Did you find any errors?
- Is the information presented?
- Do you need more information? If so, where and what level of detail?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, indicate the document title and the chapter, section, and page number (if available).

You can send comments to us in the following ways:

Email:
TechDocs@aras.com
Subject: Aras Product Documentation

Or,

Postal service:
Aras Corporation
100 Brickstone Square
Suite 100
Andover, MA 01810
Attention: Aras Technical Documentation

If you want a reply, provide your name, email address, and telephone number.

If you have usage issues with the software, visit https://www.aras.com/support/.

1 Platform Support Matrix

For the software required for Aras OAuth Registry release 32:

Aras Innovator Release	Client Operating System	Browser
32	• Windows: 10 and 11 • macOS 10.15 Catalina	• Chrome 126 • Edge • Firefox: 102 ESR, 115 ESR, and 128 ESR

2 Key Features and Known Issues

2.1 Key Features in Aras OAuth Registry 32

The OAuth Registry platform component enables administrators to configure OAuth Clients within Aras Innovator. With this functionality, administrators no longer need to access the code tree and manually modify configuration files.

The following key features are available in this initial release of the Aras OAuth Registry platform component:

2.1.1 Supported Grant Types

Grant types describe how a client retrieves an access token that authorizes requests to a server. This standard OAuth 2.0 capability enables Aras Innovator administrators to configure OAuth Clients that support a variety of use cases and security levels.

This release includes the following grant types:

- Authorization Code: The user agent requests an authorization code from the Aras Innovator OAuth server. The authorization code is then sent to the server-side client, which can exchange it for an access token.
- Implicit: The client redirects the user to the Aras Innovator login page, where they enter their credentials. After the login succeeds, the client receives an access token directly. This is commonly used for cases with thin clients without server-side components, such as Single Page Applications.
- Impersonate: The client uses a certificate to request an access token from the OAuth Server for a given user. The access token can then be used to send requests on behalf of the associated user. All requests sent with this access token will be executed as the specified Aras Innovator user. This is typically used for integrations and server-to-server use cases without end-user interaction.
- Password: The client exchanges a user's credentials for an access token. This grant type is typically not recommended because the client application must collect the user's password and send it to the authorization server.

2.1.2 Token Lifetime Settings

These settings enable administrators to limit the time that access and refresh tokens are valid. This ensures that tokens may not be used indefinitely.

2.1.3 Logout URLs

These settings provide support for applications requiring back-channel logout and front-channel logout.

2.1.4 Allowed Scopes

This setting enables administrators to specify the scope(s) that an OAuth Client may request. OAuth scopes can be used to limit the data an application can access.

2.1.5 Allowed CORS Origins

This setting specifies a list of domains the client may use to send requests. It supports JavaScript applications and clients that require cross-origin resource sharing (CORS).

2.1.6 Redirects

2.1.6.1 Redirect URIs

This setting specifies the universal resource identifiers (URIs) that may receive authorization codes or tokens for this client. Configuring redirect URIs prevents applications from redirecting users to unapproved sites after login.

2.1.6.2 Post Logout Redirect URIs

This setting specifies which URIs to redirect to after logout. Configuring redirect URIs prevents applications from redirecting users to unapproved sites after logout.

2.1.7 Secrets

2.1.7.1 Plain Secrets

This setting specifies a plain text string the OAuth client can include in requests. Plain Secrets can provide an extra layer of security for OAuth Clients.

2.1.7.2 Certificate Secrets

This setting specifies a Base64 encoded certificate containing the OAuth Client's public key. Certificate Secrets can provide an extra layer of security for OAuth Clients.

2.2 Known Issues in Aras OAuth Registry 32

Issue #	Description	Workaround
I-065444	Selecting "Authorization Code" under Allowed Grant Types may incorrectly show a "required" validation message.	Select "Authorization Code" a second time and the validation message will disappear.
I-065853	When a user tries to save an empty OAuth Client form, an error message appears: "ClientID cannot be null or empty."	Delete the empty item instead of saving it.