



OAuth2 Provider

[Save](#) [Reset](#) [Back to Services](#)

* Indicates required field

Realm Attributes

* Authorization Code Lifetime (seconds):

* Refresh Token Lifetime (seconds):

* Access Token Lifetime (seconds):

Issue Refresh Tokens: Enabled

Issue Refresh Tokens on Refreshing Access Tokens: Enabled

Custom Login URL Template:

A Freemarker template which will create a custom URL for the login page to authenticate the resource owner. The following values are available to the Freemarker template: gotoUrl - the URL to redirect back to the OAuth2 authorization process, acrValues - the acr values for the OAuth2 authorization request, realm - the OpenAM realm the OAuth2 authorization request was made on, module - the name of the OpenAM authentication module requested to perform resource owner authentication, service - the name of the OpenAM authentication chain requested to perform resource owner authentication, locale - a space separated list of locales ordered by preference.

* Scope Implementation Class:

Response Type Plugins

Current Values	<input type="text" value="id_tokenorg.forgerock.restlet.ext.oauth2.flow.responseTypes.IDTokenResponseType"/> <input type="text" value="tokenorg.forgerock.restlet.ext.oauth2.flow.responseTypes.TokenResponseType"/> <input type="text" value="codeorg.forgerock.restlet.ext.oauth2.flow.responseTypes.CodeResponseType"/>	Remove
----------------	--	------------------------

New Value [Add](#)

Response types are input as such, codelname of plugin class. For example, codelorg.forgerock.openam.oauth2.CodeClass. If there is no implementation class none should be used in place of the class name. For example id_tokenInone.

User Profile Attribute(s) the Resource Owner is Authenticated On

Current Values [Remove](#)

uid cn openid profile

New Value

If the attribute is mail and uid, then a search string of `!(mail=user)(uid=user)` will be used to get the user profile, where user is the username entered during authentication.

Saved Consent Attribute Name:

To use saved consent a list attribute must be set up and the attribute name provided.

Remote JSON Web Key URL:

The Remote URL where the providers JSON Web Key can be retrieved.

Subject Types supported

Current Values	public	<input type="button" value="Remove"/>

New Value

List of subject types supported. Values are pairwise and public. Pairwise is the same as confidential.

ID Token Signing Algorithms supported

Current Values	HS256 HS512 RS256 HS384	<input type="button" value="Remove"/>

New Value

Algorithms supported to sign id_tokens.

Supported Claims

Current Values	<input type="button" value="Remove"/>
----------------	---------------------------------------

phone email address openid profile

New Value

List of claims supported by the userinfo endpoint.

* **OpenID Connect JWT Token Lifetime (seconds):**
The amount of time in seconds the JWT will be valid for.

* **Alias of ID Token Signing Key:**
The name of the key put in the keystore used to sign the ID Tokens issued by OpenAM.

Allow Open Dynamic Client Registration: Enabled
Allow clients to register without an access token. If enabled, you should consider adding some form of rate limiting. See [Client Registration](#) in the OpenID Connect specification for details.

Generate Registration Access Tokens: Enabled
Whether to generate Registration Access Tokens for clients that register via open dynamic client registration. Such tokens allow the client to access the [Client Configuration Endpoint](#) as per the OpenID Connect specification. This setting has no effect if open dynamic client registration is disabled.

OpenID Connect acr_values to Auth Chain Mapping

Current Values

--

New Value

Map Key	Corresponding Map Value
<input type="text"/>	<input type="text" value="[Empty]"/> <input type="button" value="Add"/>

Maps OpenID Connect ACR values to authentication chains. See [the acr_values parameter](#) in the OpenID Connect authentication request specification for more details.

OpenID Connect default acr claim:
Default value to use as the 'acr' claim in an OpenID Connect ID Token when using the default authentication chain.

OpenID Connect id_token amr values to Auth Module mappings

Current Values

New Value	Map Key	Corresponding Map Value
	<input type="text"/>	<input type="text" value="DataStore"/> <input type="button" value="Add"/>

If you require `amr` values to be returned in the OpenID Connect `id_token`, you can configure them here. Once authentication has completed, the authentication modules that were used from the authentication service will be mapped to the `amr` values. If you do not require `amr` values, or are not providing OpenID Connect tokens at all, this field can be left blank.

Modified Timestamp attribute name:

The attribute name of the modified timestamp in the identity repository (must also be added to the User Attributes List on the Datastore Service page).

Created Timestamp attribute name:

The attribute name of the created timestamp in the identity repository (must also be added to the User Attributes List on the Datastore Service page).