VERSION LOG OUT

User: amAdmin Server: sp.example.com

FORGEROCK

OAuth2 Provider

Save Reset Back to Services

* Indicates required field

Realm Attributes

*** Authorization Code Lifetime (seconds):**
120
The time in seconds an authorization code is valid for

*** Refresh Token Lifetime (seconds) If this field is set to -1, the token will never expire.:**
604800
The time in seconds a refresh token is valid for

*** Access Token Lifetime (seconds):**
3600
The time in seconds an access token is valid for

Issue Refresh Tokens:
Enabled
Check to enable generation of refresh tokens

Issue Refresh Tokens on Refreshing Access Tokens:
Enabled
Check to enable generation of refresh tokens when refreshing access tokens

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:**
org.forgerock.openam.oauth2.OpenAMScope\
The class that contains the required scope implementation

OIDC Claims Script.:
OIDC Claims Script Refresh
This is a script that will be run, when using an implementation of the org.forgerock.openam.oauth2.OpenAMScopeValidator, when issuing an ID Token or making a request to the userinfo endpoint that will gather and fill in all claims for the request. The script has access to the requested scopes, the access token, the user's session (if available), the user's identity.

Create Edit

Response Type Plugins

Current Values
tokenlorg.forgerock.restlet.ext.oauth2.flow.responseTypes.TokenResponseType
codelorg.forgerock.restlet.ext.oauth2.flow.responseTypes.CodeResponseType
Remove

New Value
Add

Response types are input as such, codeIname 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

uid
cn
openid
profile

Remove

New Value Add

If the attribute is mail and uid, then a search string of (I(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.

User Display Name attribute: cn

The attribute for identities retrieved from the ID Repository that contains a displayable name for the user for use in the consent page.

Supported Scopes

Current Values

cn
openid
profile

Remove

New Value Add

A list of scopes this authorization server supports, with translations.

Remote JSON Web Key URL:

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

Subject Types supported

Current Values

public

Remove

New Value Add

List of subject types supported. Valid values are pairwise and public.

ID Token Signing Algorithms supported

Current Values

HS256
RS256

Remove

New Value

Add

Algorithms supported to sign id_tokens.

Supported Claims

Current Values

phone
email
address
openid
profile

Remove

New Value

Add

List of claims supported by the userinfo endpoint, with translations.

*** OpenID Connect JWT Token Lifetime (seconds):**

3600

The amount of time in seconds the JWT will be valid for.

*** Alias of ID Token Signing Key:**

test

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

Remove

	Map Key	Corresponding Map Value	
New Value		[Empty]	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 Remove

	Map Key	Corresponding Map Value	
New Value		DataStore	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).

Default Client Scopes

Current Values Remove

cn
openid
profile

New Value Add

List of scopes a client will be granted if they request registration without specifying which scopes they want. Default scopes are NOT auto-granted to clients created through the administrator interface.

Enable "claims_parameter_supported": Enabled

If enabled, clients will be able to request individual claims using the "claims" Request Parameter as per section 5.5 of the OpenID Connect specification.

Subject identifier hash salt: changeme

If pairwise subject types are supported, it is STRONGLY RECOMMENDED to set this value. It is used in the salting of hashes for returning specific sub claims to individuals using the same request_uri or sector_identifier_uri.

Always return claims in ID Tokens:

☐ Enabled

All id_tokens will contain scope-derived claims. Warning: not strictly spec-compliant.

Code verifier parameter required:

☐ Enabled

If enabled, Authorization Code requests will require a "code_challenge" attribute

Verification URL:

The URL that the user will be instructed to visit to complete their OAuth 2 login and consent when using the device code flow.

Device Completion URL:

The URL that the user will be sent to on completion of their OAuth 2 login and consent when using the device code flow.

Device Code Lifetime (seconds):

300

The lifetime of the device code.

Device Polling Interval:

5

The polling frequency for devices waiting for tokens when using the device code flow.

Save | Reset | Back to Services