User: amAdmin Server: sp.example.com



OAuth2 Provid	er Save Reset Back to Services
	* Indicates required field
Realm Attribut	es
* Authorization Code Lifetime (seconds):	6000
* Refresh Token Lifetime (seconds):	6000
* Access Token Lifetime (seconds):	6000
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:	org.forgerock.openam.oauth2.OpenAMScope\
Response Type F	Plugins
Current Values	id_tokenlorg.forgerock.restlet.ext.oauth2.flow.responseTypes.IDTokenResponseType tokenlorg.forgerock.restlet.ext.oauth2.flow.responseTypes.TokenResponseType codelorg.forgerock.restlet.ext.oauth2.flow.responseTypes.CodeResponseType
New Valu	e Add

If there is no implementation class none should be used in place of the class name. For example id_tokenInone.

Response types are input as such, codelname of plugin class. For example, codelorg.forgerock.openam.oauth2.CodeClass.

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

Current Values

Remove

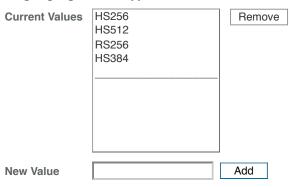
	uid cn openid profile	
New Value		Add

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.
Remote JSON Web Key U	
	The Remote URL where the providers JSON Web Key can be retrieved.
Subject Types supported	
Current Values	public Remove
-	
L	
New Value	Add

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

ID Token Signing Algorithms supported



Algorithms supported to sign id_tokens.

Supported Claims

Current Values Remove

	openid profile		
New Value	Add		
List of claim	s 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 conside See Client Registration in the OpenID Connect specification for details.	er adding some form of rate limiting.	
Generate Registration Access Tokens:	✓ Enabled Whether to generate Registration Access Tokens for clients that register via optokens allow the client to access the Client Configuration Endpoint as per the setting has no effect if open dynamic client registration is disabled.		
OpenID Connect a	cr_values to Auth Chain Mapping		
Current Va	Remove		
New Value	Map Key Corresponding Map Value [Empty] Add		
	D Connect ACR values to authentication chains. See the acr_values paramer on request specification for more details.	ter in the OpenID Connect	
OpenID Connect of claim:	Default value to use as the 'acr' claim in an OpenID Connect ID authentication chain.	Token when using the default	

Remove

phone email address

OpenID Connect id_token amr values to Auth Module mappings

Current Values



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:

modifyTimestamp

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:

createTimestamp

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).

Save Reset Back to Services