



Edit http://sp.example.com:8080/openam

Save

Reset

Back to Main Page

Inheritance Settings

Export Configuration

* Indicates required field

Group: [None] ▾

* Status: ☒ Active
☐ Inactive

Status of the agent configuration.

* Client password:

Client password. Used when the client authenticates to OpenAM.

* Client password (confirm): * Client type: ☒ Confidential
☐ Public

Type of OAuth 2.0 client. Confidential clients can keep their password secret, and are typically web apps or other server-based clients. Public clients run the risk of exposing their password to a host or user agent, such as rich browser applications or desktop clients.

Redirection URIs

Current Values

--

Remove

New Value

Add

Redirection URIs (optional for confidential clients). Complete URIs or URIs consisting of protocol + authority + path are registered so that the OAuth 2.0 provider can trust that tokens are sent to trusted entities. If multiple URI's are registered, the client MUST specify the URI that the user should be redirected to following approval. May not contain a fragment (#).

Scope(s)


Current Values

cn openid profile

Remove


New Value

Add

 Scope(s). Scopes are strings that are presented to the user for approval and included in tokens so that the protected resource may make decisions about what to give access to.


Claim(s)

Current Values	<div></div>	Remove
New Value	<div></div>	Add

 List of claim name translations, which will override those specified for the AS. Claims are values that are presented to the user to inform them what data is being made available to the Client.


Display name

Current Values	<div></div>	Remove
New Value	<div></div>	Add

 A client name that may be relevant to the resource owner when considering approval.

Display description

Current Values	<div></div>	Remove
New Value	<div></div>	Add

 A description of the client or other information that may be relevant to the resource owner when considering approval.

Default Scope(s)

Current Values	Remove
----------------	--------

New Value

Response Types

Response types this client will support and use.

Email addresses of users who can administrate this client.

The authentication method the token endpoint should use.

The uri that contains the client's public keys in Json Web Key format.

The Host component of this URL is used in the computation of pairwise Subject Identifiers.

The subject type added to responses for this client.

ID Token Signed Response Algorithm:

Algorithm the ID Token for this client must be signed with.

Post Logout Redirect URIs**Current Values**

New Value

URIs that can be redirected to after the client logout process.

Access Token:

The access token used to update the client.

Client Session URI:

This is the URI that will be used to check messages sent to the session management endpoints. This URI must match the origin of the message

Client Name**Current Values**

New Value

This value is a readable name for this client.

Client JWT Bearer Public Key:

A Base64 encoded X509 certificate, containing the public key, represented as a UTF-8 PEM file, of the key pair for signing the Client Bearer JWT.

Default Max Age:

Minimum value 1. Sets the maximum length of time in seconds a session may be active after the authorization service has succeeded before the user must actively re-authenticate.

Default Max Age Enabled:☐ Enabled

Whether or not the default max age is enforced.

Public key selector:

☐ JWKS
☐ JWKS_URI
☒ X509

Select the public key for this client to come from either the jwks_uri, manual jwks or X509 field.

Authorization Code Lifetime (seconds):

The time in seconds an authorization code is valid for. *NB* If this field is set to zero, Authorization Code Lifetime of the OAuth2 Provider is used instead of.

Refresh Token Lifetime (seconds):

The time in seconds a refresh token is valid for. *NB* If this field is set to zero, Refresh Token Lifetime of the OAuth2 Provider is used instead. If this field is set to -1, the token will never expire.

**Access Token Lifetime
(seconds):**

The time in seconds an access token is valid for. *NB* If this field is set to zero, Access Token Lifetime of the OAuth2 Provider is used instead of.

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

The time in seconds a JWT is valid for. *NB* If this field is set to zero, JWT Token Lifetime of the OAuth2 Provider is used instead of.