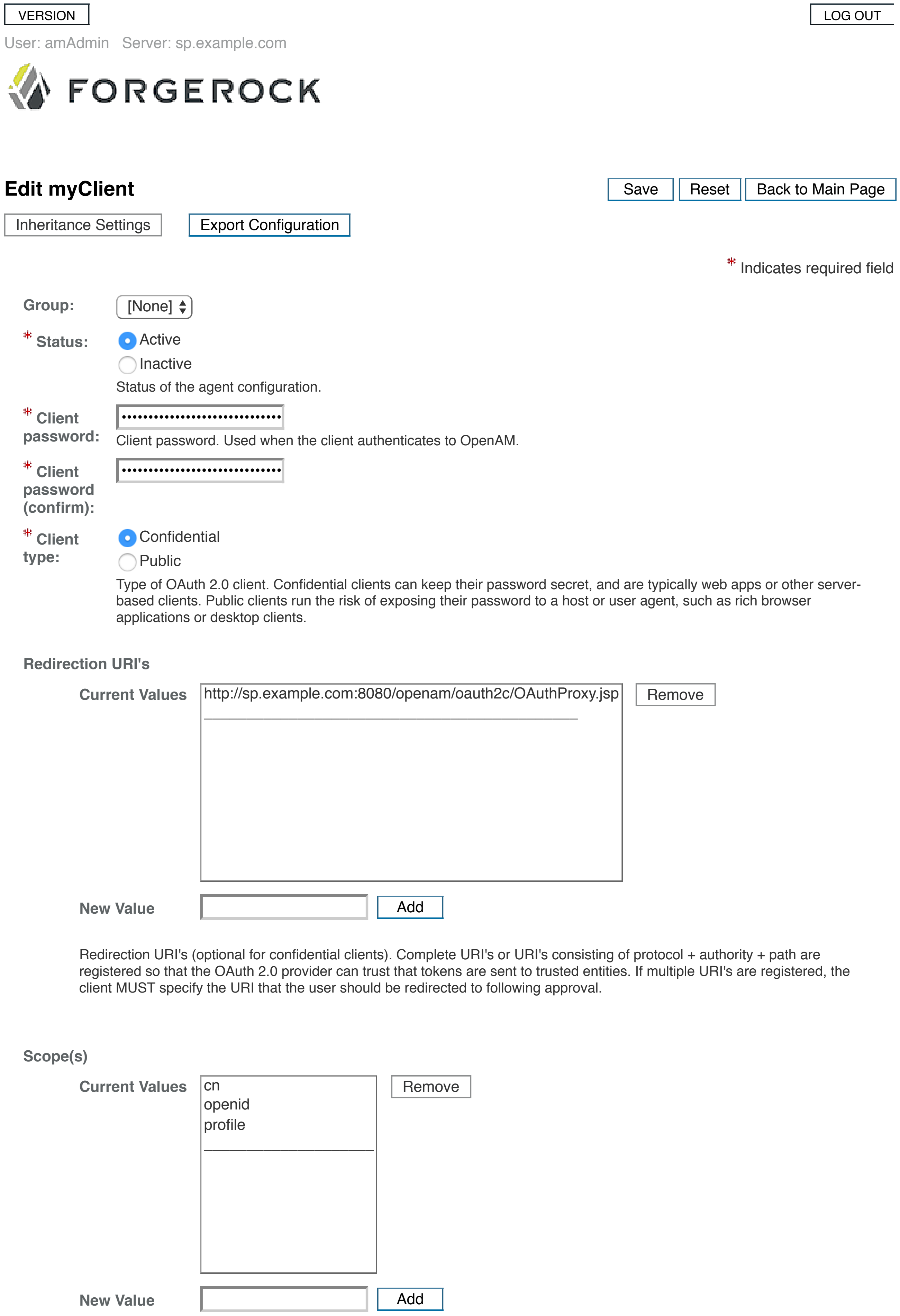

User: amAdmin Server: sp.example.com

Edit myClient

* 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 URI's

Current Values: http://sp.example.com:8080/openam/oauth2c/OAuthProxy.jsp

New Value:

Redirection URI's (optional for confidential clients). Complete URI's or URI's 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.

Scope(s)

Current Values: cn
openid
profile

New Value:

ℹ 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.

Display name

Current Values Remove

New Value Add

ℹ The name as displayed to users during approval.

Display description

Current Values Remove

New Value Add

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

Default Scope(s)

Current Values

cn
openid
profile

Remove

New Value Add

ℹ Default Scope(s). Scopes automatically given to tokens.

Response Types

Current Values Remove

code
token
id_token
code token
token id_token
code id_token
code token id_token

New Value Add

Response types this client will support and use.

Contacts

Current Values Remove

New Value Add

Email addresses of users who can administrate this client.

ID Token Signed Response Algorithm: HS256

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

Post Logout Redirect URI:

The URI to redirect 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:

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.

Authorization Code Lifetime (seconds): 0

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.

Refresh Token Lifetime (seconds): 0

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.

Access Token Lifetime (seconds): 0

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.

OpenID Connect JWT Token Lifetime (seconds): 0

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.