

Gluu Identity and Access Management Platform

How to setup gluu

1. follow all the screen shots in the folder, and fill all fields as they are in the screen shots
 2. the next step is to configure custom attribute, in our case we configure the role attribute and we assign this attribute to the openid scope
- How to configure the roles to work:

1. You need to make sure all your custom attributes have "Usage Type" set to "OpenID" and assigned some "OAuth claim name".
2. Then you need to add these attributes to some scopes at "OpenID Connect -> Scopes", either to a pre-packaged one, or create a custom scope as well. In our case add it to the openid.
3. If you need your client to request for this scope during dynamic registration, make sure you'll set "Allow for dynamic registration" flag for this scope.

The screenshot shows the 'OpenID Connect - Update Client' configuration page. The left sidebar contains navigation options: Configuration, SAML, OpenID Connect, Scopes, Clients, Single Identifier, UMA, Users, and Personal. The main content area is titled 'Client Config Summary' and includes a 'Delete' button. It features tabs for 'Standard settings', 'Advanced settings', and 'Encryption/Signing settings'. The 'Advanced settings' tab is active, showing fields for Client ID, Client Secret, Client Name (set to 'iDP client'), Client Description, Disabled (unchecked), Redirect Login URIs, Scopes (openid, user_name, email), Response Types (code), Grant Types (authorization_code, refresh_token), Pre-authorization, Persist Client Authorizations, Application Type (Web), Subject Type (public), Authentication method for the Token Endpoint (client_secret_basic), and Client's Registration Expires (calendar view for December 2019). There are also fields for Logo URI and Policy URI.

The screenshot shows the 'Attributes - Edit Attribute' configuration page. The left sidebar is the same as the previous screenshot. The main content area is titled 'Attributes - Edit Attribute' and includes an 'Edit Attributes' button. It features fields for Name (role), SAML URI, Display Name (User Permission), Type (Text), Edit Type (select), View Type (select), Usage Type (Not defined), Multivalued (True), OAuth claim name (role), SCIM Attribute (glu:Permission), Description (glu:Permission), Enable custom validation for this attribute (checked), Validation RegEx, Enable lookup for this attribute (unchecked), Minimum Length, Maximum Length, Regex Pattern, and Status (Active). There are 'Update', 'Delete', and 'Cancel' buttons at the bottom.

The screenshot shows the 'OpenID Connect - Update Scope' configuration page. The left sidebar is the same as the previous screenshots. The main content area is titled 'OpenID Connect - Update Scope' and includes an 'Update Scope' button. It features fields for ID Name, Display Name (openid), Description (Authenticate using OpenID Connect), Scope Type (OpenID), and Allow for dynamic registration (True). The 'Claims' section lists various attributes with checkboxes: Display Name, Email, First Name, Gender: male or female, Name, Inum, Last Name, Locale, Username, and User Permission. There is an 'Add Claim' button and 'Update', 'Delete', and 'Cancel' buttons at the bottom.

Client Config Summary Delete

Standard settings **Advanced settings** Encryption/Signing settings

Access Token as JWT: Require Auth Time:

RPT as JWT: Include Claims in Id Token:

Logout Session Required:

Claim Redirect URIs:

Request URIs:

Authorized JavaScript Origins:

Contacts:

Front Channel Logout URI:

Default requested Authentication Context Class Reference (ACR) values:

Client URI:

Terms of Service URI:

ID Token Binding Confirmation Method:

Sector Identifier URI:

Initiate Login URI:

Refresh Token Lifetime:

oid Id:

Default Maximum Authentication Age:

Access Token Lifetime:

Software Identifier:

Software Version:

User

memberOf:

Middle Name:

Nickname:

Phone Number Verified:

Picture URL:

Preferred Username:

Profile URL:

Time zone info:

User Permission: + Click on the + to add new User Permission

User Permission 1:

User Permission 2:

User Status:

Username:

Website URL:

Change Password Update Delete Cancel

gluu English

GLUU Identity Appliance **OpenID Connect** Update Client Update Client

Client Config Summary Delete

Standard settings **Advanced settings** Encryption/Signing settings

JWE alg Algorithm for encrypting Request Objects:

JWE enc Algorithm for encrypting Request Objects:

JWS alg Algorithm for signing Request Objects:

JWE alg Algorithm for encrypting the UserInfo Responses:

JWE enc Algorithm for encrypting the UserInfo Responses:

JWS alg Algorithm for signing the UserInfo Responses:

JWKS URI:

JWKS:

Access Token signing algorithm:

JWE alg Algorithm for encrypting the ID Token:

JWS alg Algorithm for signing the ID Token:

JWE enc Algorithm for encrypting the ID Token:

JWS alg Algorithm for Authentication method to Token Endpoint:

Update Cancel



- Configuration
- SAML
- Trust Relationships
- Add Trust Relationships
- Configure Custom NameId
- OpenID Connect
- UMA
- Users
- Personal

Enabled:	<input checked="" type="checkbox"/>	Delete NameId
Source Attribute:	<input type="text" value="Email"/>	
Name:	<input type="text" value="emailAddress"/>	
NameId Type:	<input type="text" value="emailAddress"/>	

[Add NameId configuration](#)[Update](#) [Cancel](#)