Cloud Native Identity

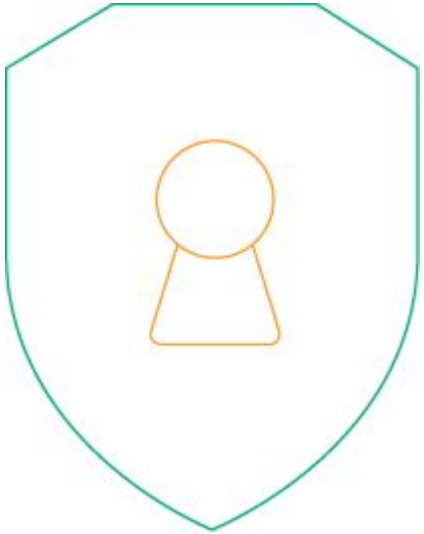
How to build a world-class identity service with Gluu

https://gluu.org @gluufederation https://github.com/GluuFederation

What is Gluu?

Gluu is a free open source software platform for identity & access management that helps you:

- Achieve single sign-on (SSO)
- Authenticate citizens
- Rollout multi-factor authentication (MFA)
- Secure access to websites & APIs



A little bit about us...

45+

Team members around the world

11+

Years active development

100+

Enterprise customers

3,000+

Deployments per year

20+

Global services partner organizations

1 mission:

Create the best IAM platform in the world.

gluu

We work with...


esa
European Space Agency


CenturyLink™


Cognizant


TELE2


Ville de Montréal


Canada


Evernote


Invesco


gluu

Products

Gluu Server

Central service that authenticates users and issues tokens

Gluu Gateway

HTTP reverse proxy to secure web sites & APIs

Casa

User portal for self-service 2FA management

Super Gluu

Mobile app for 2FA

Value Proposition

Very flexible

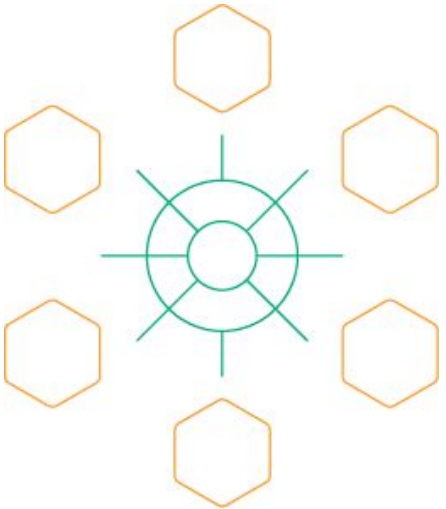
Multi-step authentication and authorization workflows

Hyper-scalability

Any number of users. Any concurrency.

Open web standards

Avoid lock-in with open standard interfaces:
OpenID, OAuth, SAML, FIDO, UMA, SCIM



gluu

Origins

2011

- oxAuth is born! Required for a project with ID^3 Institute at MIT Media Lab

2013

- Even before self-certification program, Gluu leads interop 4

OpenID Connect Provider Test Results

Here is a summary of the implementations that are tested using Federation Lab, and an update on what tests that succeeded and not.

Test flows	oic.info	heroku	RH	orange	oic4us	gluu
Rejects redirect_uri when Query Parameter Does Not Match			✓	✓		✓
Flow with response_type='code token idtoken'	✓	✓	✓	✓	✓	✓
Flow with response_type='code idtoken token' grab a second token using the code and then do a Userinfo request	✓	✓	✓	✓	✓	✓
Request with display=popup	✓	✓	✓	✓	✓	✓
Can Provide Encrypted ID Token Response						!
RP wants symmetric IdToken signature				!		✓
Access token request with public_key_jwt authentication			✓	!		✓
Authorization request missing the 'response_type' parameter			✓	✓		✓
using prompt=none with user hint through IdToken				✓		✓
RP wants signed UserInfo returned				!		✓
Scope Requesting all Claims	✓	✓	✓	✓	✓	✓
OpenID Request Object with Required name Claim	!	!	✓	!	!	✓

Excerpt from Interop results from 1/7/2013

gluu

Gluu has a long record of excellent results

- Gluu (oxAuth) is the only implementation to recertify four times: **2015, 2017, 2018, 2019**

Organization	Implementation	Basic OP	Implicit OP	Hybrid OP	Config OP	Dynamic OP	Form Post OP	3rd Party-Init OP
Gluu	Gluu Server 4.0.0	15-Oct-2019	15-Oct-2019	15-Oct-2019	15-Oct-2019	15-Oct-2019	15-Oct-2019	22-Oct-2019

Certified Financial-grade API (FAPI) OpenID Providers

Organization	Implementation	FAPI R/W OP w/ MTLS	FAPI R/W OP w/ Private Key
Gluu	Gluu Server 4.2	20-Feb-2020 [view]	20-Feb-2020 [view]

https://openid.net/certification

OpenID Connect

oxAuth implements:

- OpenID Core
- Dynamic Client Registration
- Discovery
- Session Mgt, Front/Back Channel Logout
- Form Post Response Mode
- Client Initiated Back Channel Authentication (4.2)

FIDO

Set of standards to implement phishing resistant authentication

- FIDO U2F: older protocol for USB keys, but useful for other situations where you need public key enrollment and a challenge / response authentication protocol (e.g. mobile app “Super Gluu” uses FIDO U2F endpoints)
- FIDO 2: combination of W3C Web Authn + CTAP. Widely supported by browsers including Apple, Microsoft, Google.
- FIDO U2F and FIDO 2 endpoints
- Currently in oxAuth, but could be moved to separate microservice

SCIM 2.0

API for user management (i.e. Add User, Edit User, Delete User, Search Users)

- RFC 7643 : SCIM Core Schema
- RFC 7644 : SCIM Core protocol
- Interoped with Sailpoint, Ping and others
- Did not implement ‘eTags’ due to lack of customer requests for feature (it’s a MAY in the spec) https://tools.ietf.org/html/rfc7644#section-3.14
- Currently implemented in oxTrust, but code will be moved to stand alone microservice

UMA

Kantara User Managed Access Profile version 2.0

- Protocol useful when user interaction is required post-authentication
- “Federated authorization”
- oxAuth is the most comprehensive implementation of the protocol
- Other vendors which support UMA include Forgerock, Red Hat Keycloak and WS02

Other OpenID / OAuth Features

- Support for both value (i.e. JWT) and reference access tokens
- Persistent pairwise identifiers (not just algorithmic)
- Pre-authorization of trust (i.e. suppress Open Consent for trusted clients)
- PKCE (used for mobile and Javascript clients)
- Dynamic OpenID Scopes (calls interception script)
- Spontaneous Scopes (use regular expressions to describe scopes) -- useful in cases where scope follows pattern, like a transaction id.
- Include claims in id_token (like SAML assertion)
- Private key authentication at token endpoint (asymmetric secret)

Building your identity service

Deploy Casa for “self-service 2FA”

Improve the UX for 2FA with Casa, a self-service dashboard for users to:

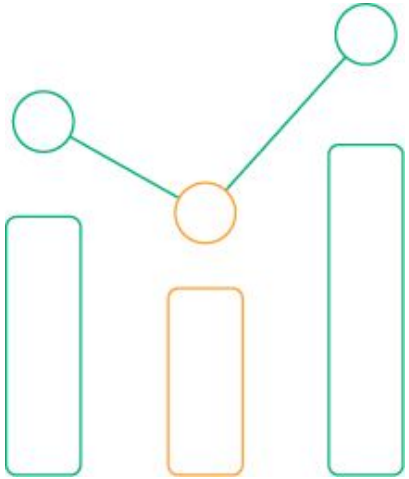
- Enroll & delete 2FA credentials--FIDO keys, OTP apps, SMS phone numbers and more.
- Manage “account linking” with external identity providers (e.g. social networks)
- View and revoke previously granted OAuth consent decisions

gluu

Scaling up

Now that you've built a fully functional identity service… it's time to scale up! Consider the following questions:

- How large is your user base?
- What's your desired performance for TPS?
- What's your operational preference: VM's or containers?



gluu

Scaling up

DB Considerations

Performance is largely driven by the DB. Gluu supports two options: LDAP or Couchbase EE.

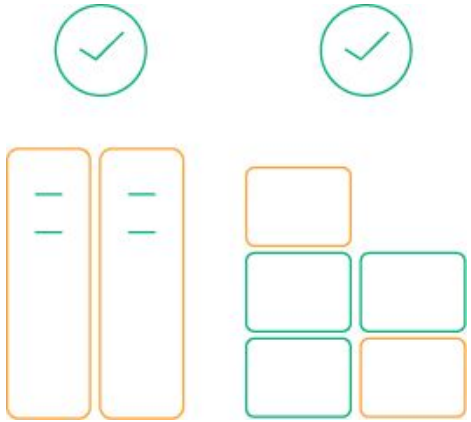
- Use **LDAP** if your data can fit into one server.
- Use **Couchbase** if you need sharding, support for multi-region topologies, horizontal scalability, and better business intelligence capabilities.

Scaling up

Operational Considerations

How you deploy will impact how you scale. Gluu supports two HA strategies: VMs or Kubernetes

- Use **VMs** and Community Edition (“CE”) if failover and deployment simplicity are more important than performance and elasticity.
- Use **Kubernetes** and Cloud Native Edition (“CN”) if you need auto-scaling, enhanced security, and more operational leverage.



gluu

https://gluu.org