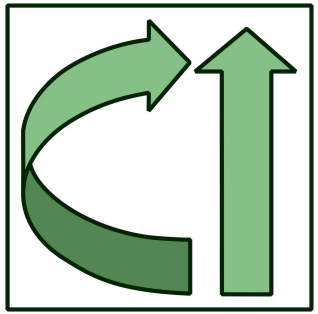


CILogon

Enabling Federated Identity and Access Management for Scientific Collaborations

Jim Basney <jbasney@ncsa.illinois.edu>
Scott Koranda <skoranda@ncsa.illinois.edu>

July 2021 IAM Online

UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN NCSA

IAM for Research Collaborations

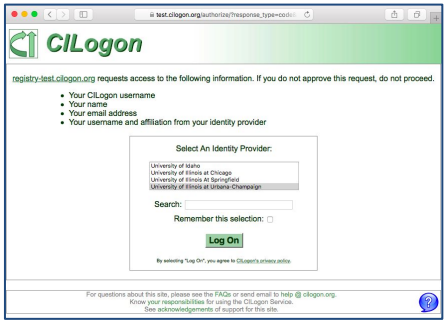
CILogon: 10+ year sustained effort to enable secure logon to scientific cyberinfrastructure (CI)

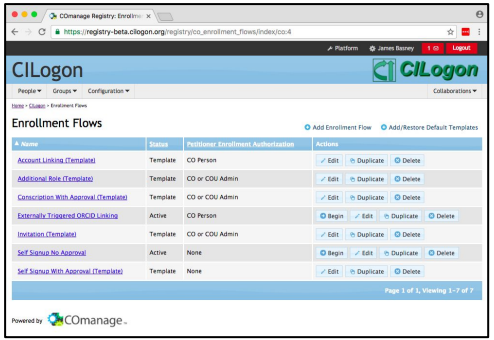
for seamless identity and access management (IAM)

using federated identities (SAML, OIDC, OAuth, JWT, X.509, LDAP, SSH, etc.) so researchers log on with their existing credentials from their home organization

supporting 12,000+ active users from 400+ organizations around the world

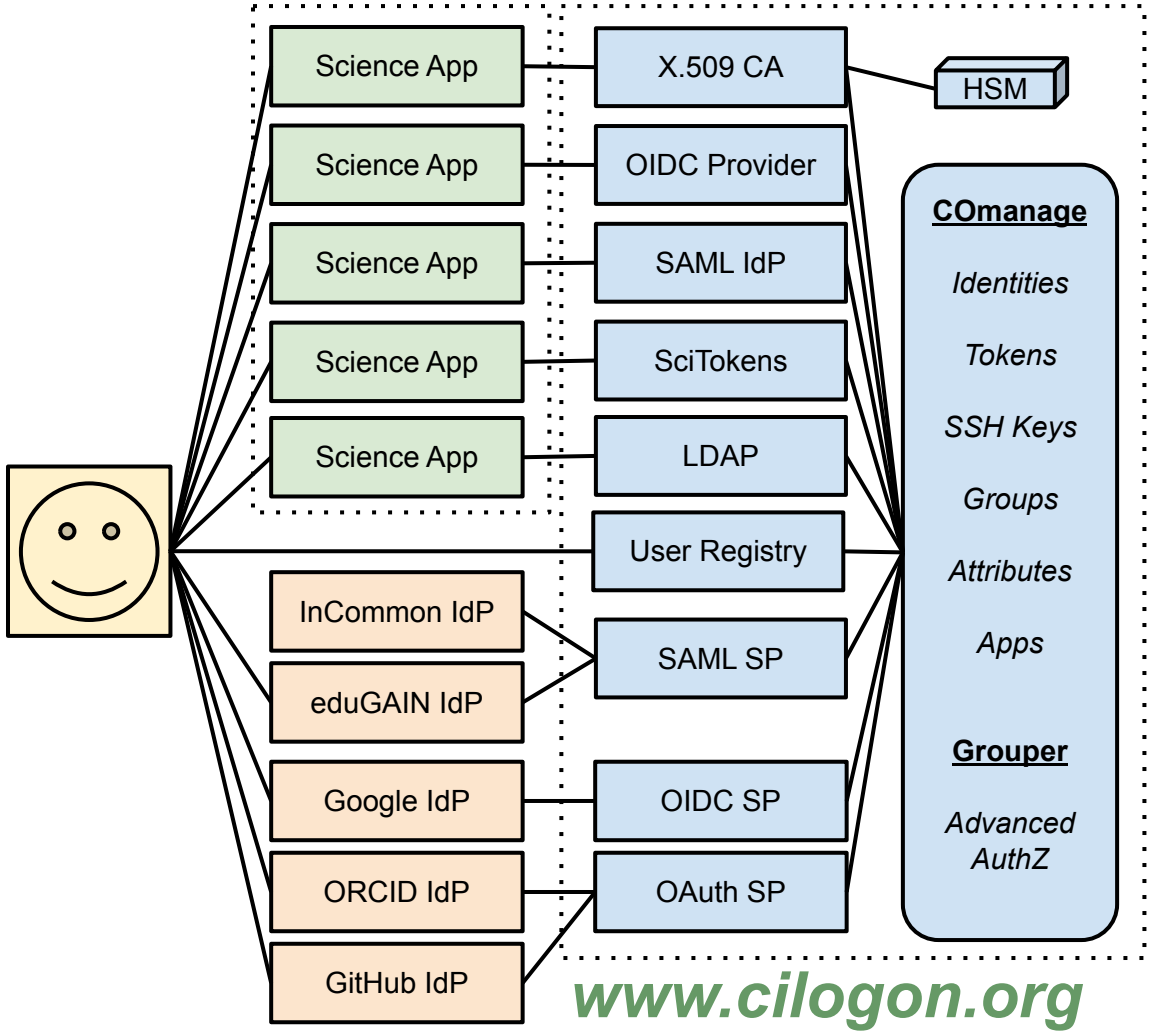
with onboarding/offboarding/attributes/groups/roles managed consistently across multiple applications





supporting access to science applications on HPC clusters, in Jupyter notebooks, using Globus, via REST APIs, and many other interfaces

using existing identity providers from the researcher's home organization (SAML/ADFS) or external sources (Google, ORCID, GitHub)



realizing our vision

align with InCommon Trusted Access Platform

- (https://www.incommon.org/trusted-access/)
- Shibboleth, COmanage, Grouper

provide hosted services

- common IAM platform across many collaborations
- growing CILogon operations (since 2010)
- reliability / sustainability

Open Source

CILogon (https://github.com/cilogon)

- OpenID Connect, OAuth, X.509

InCommon (https://www.incommon.org/trusted-access/)

- Shibboleth, COmanage, Grouper

IdentityPython (https://idpy.org/)

- pyFF, SATOSA

SciTokens (https://scitokens.org/)

OpenLDAP with voPerson (https://voperson.org)

sustainability

development supported by NSF/DOE

operational support from XSEDE

non-profit subscription model administered by NCSA/UIUC

supports long-term sustainability

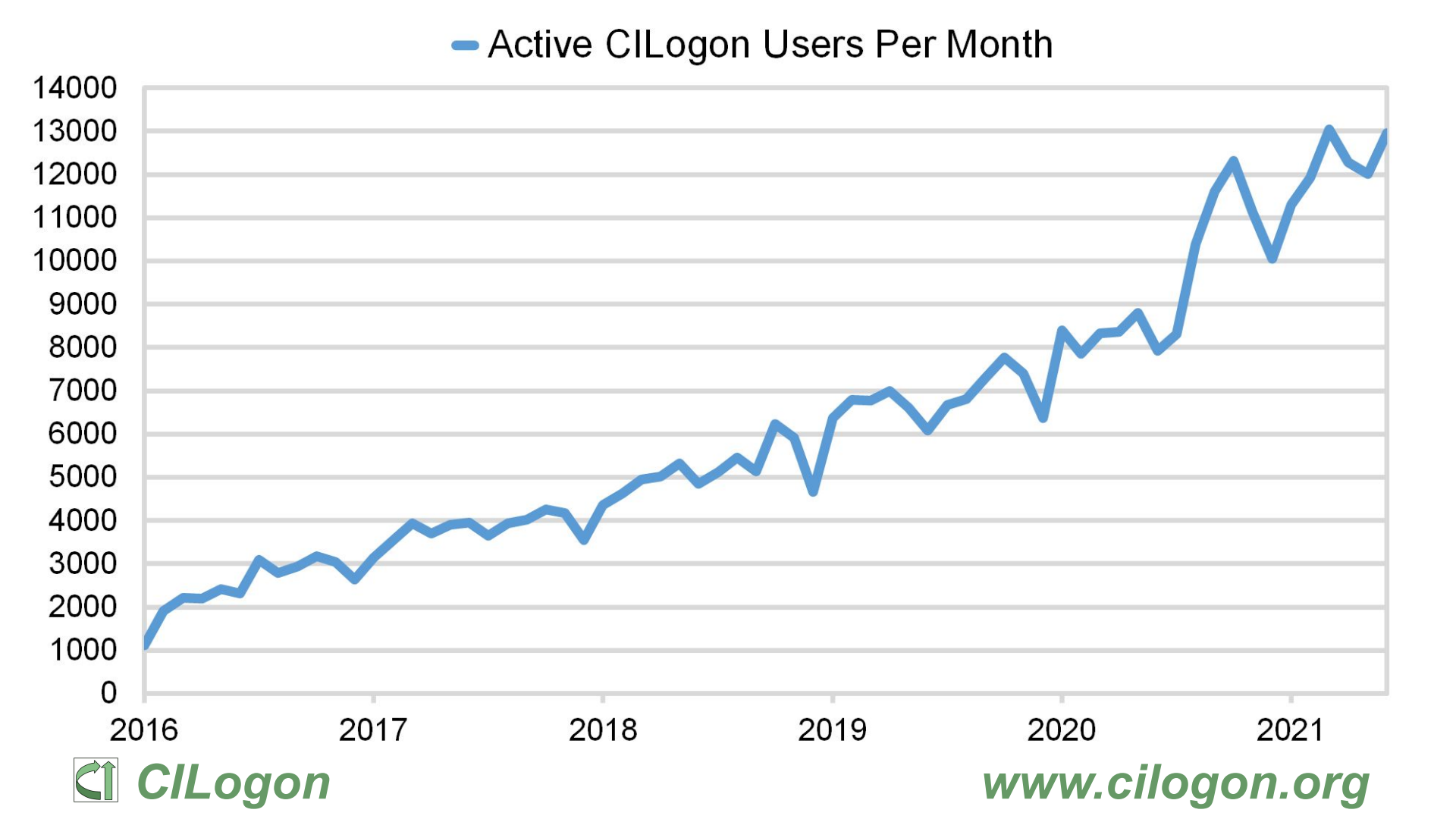
provides contracted SLAs

CILogon remains open source and focused on research & scholarship needs

https://www.cilogon.org/subscribe

our 10+ year history

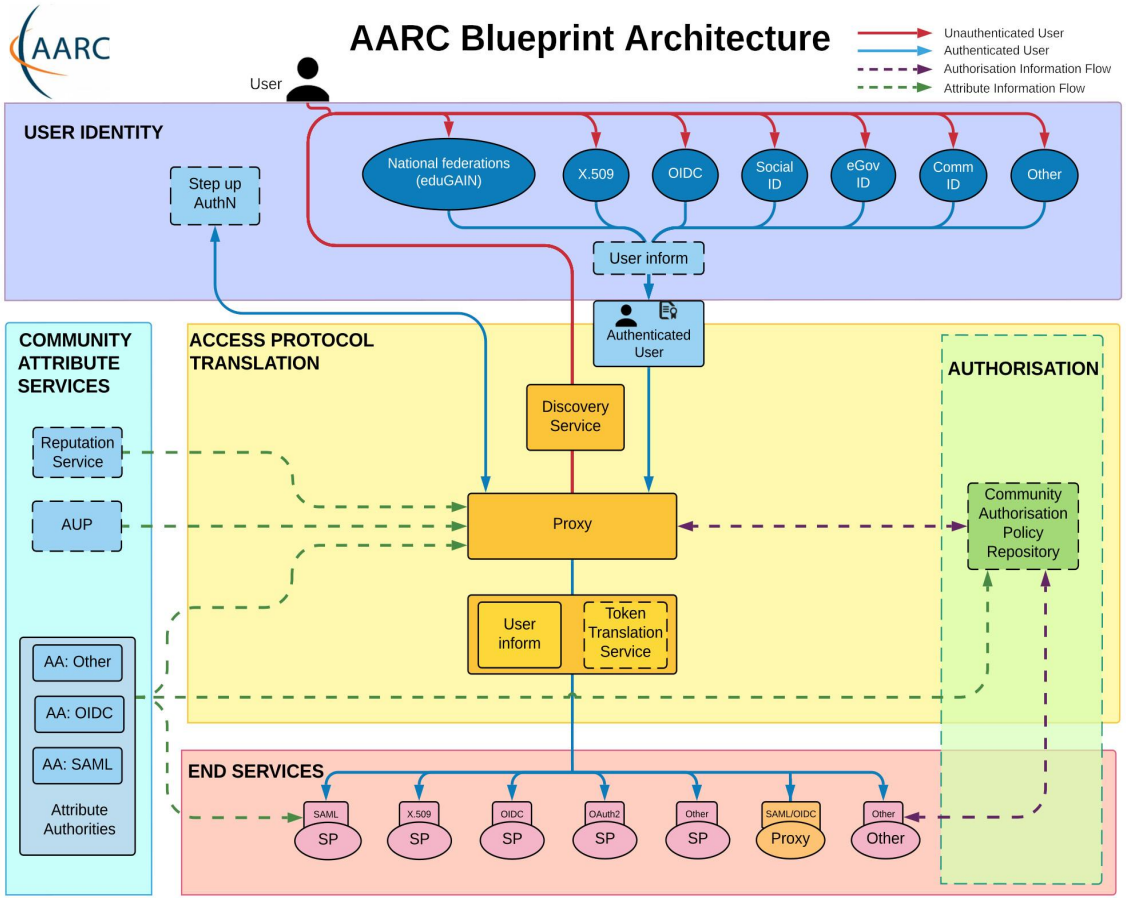
2009 Federated login to TeraGrid. NSF ARRA award.
2010 CILogon operations begin. IGTF X.509 CAs operational.
2011 NSF SDCI award. OAuth support. InCommon Silver support.
2012 DOE ASCR award. Globus identity linking. InCommon R&S.
2013 XSEDE operations support. LIGO Data Grid use.
2016 NSF CICI award. eduGAIN support. OIDC support.
2017 COmanage support. AWS deployment.
2019 Transition to subscription funding model.
2020 Grouper and SATOSA support.
2021 InCommon Catalyst Program. SciTokens and WLCG JWT support.


Active CILogon Users Per Month
14000
13000
12000
11000
10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
2016
2017
2018
2019
2020
2021
CILogon
www.cilogon.org

Top 20 IdPs

(by # of unique active users in June 2021)

638 National Institutes of Health
555 Fermi National Accelerator Laboratory
529 XSEDE
508 LIGO Scientific Collaboration
416 University of Michigan
377 University of Illinois Urbana-Champaign
335 Michigan State University
311 Penn State
249 Massachusetts Institute of Technology
238 University of Chicago
226 Purdue University Main Campus
215 Yale University
208 Stanford University
208 NCSA
194 University of California-Los Angeles
181 University of California-San Diego
163 Johns Hopkins
155 Northwestern University
153 Northeastern University
149 University of North Carolina Chapel Hill



https://aarc-community.org/architecture/

federation proxy

apps don’t need to handle the complexities of federation in isolation

many apps can’t handle 1000s of identity providers (e.g., AWS)

a federation proxy service can handle federation for many (related) apps

a federation proxy can handle targeted user identifiers consistently

open source software for operating your own proxy:

SATOSA / SimpleSAMLphp

proxy as-a-service providers:

CILogon / eduTEAMS / Globus

campus & researcher IDs

4,000+ identity providers available via eduGAIN

including CERN, NCSA, LIGO, XSEDE, ...

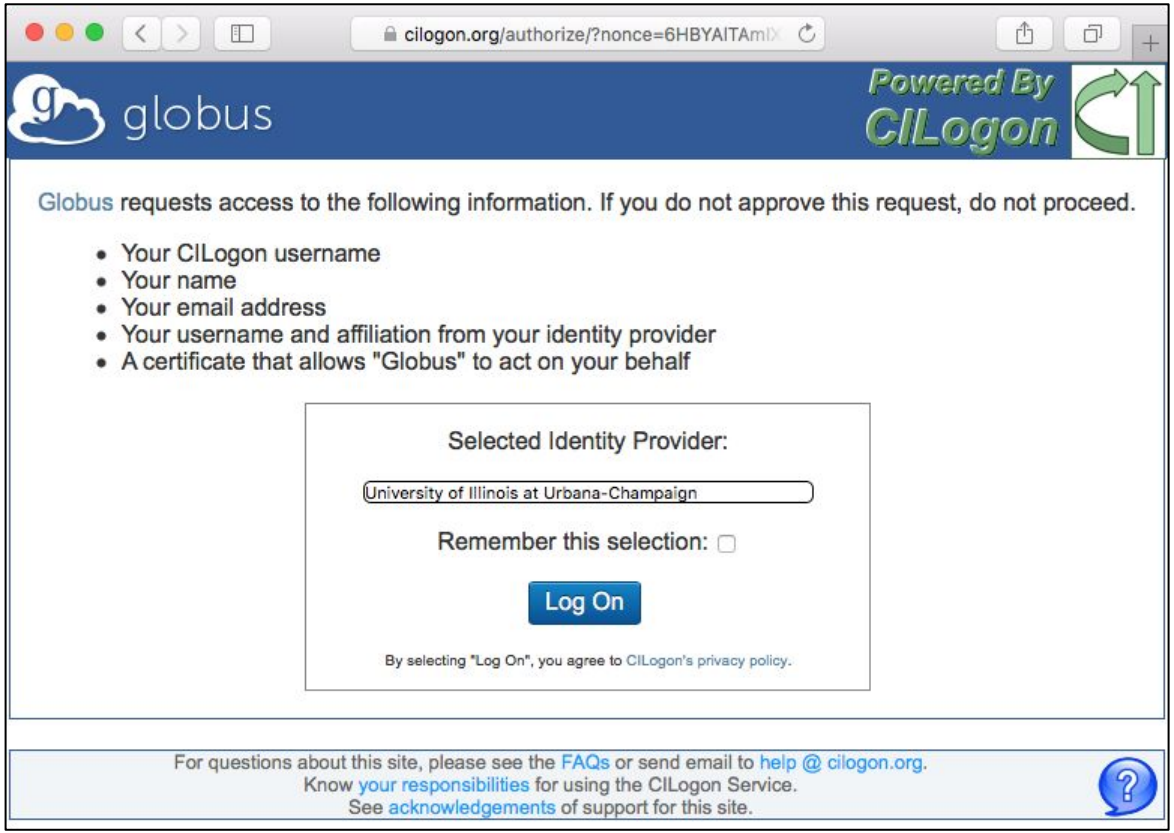
OAuth-based identity providers

ORCID GitHub Google

supporting researcher mobility

supporting researchers w/o campus IdPs

informed consent



tokens for science

WLCG Common JWT Profiles
(https://doi.org/10.5281/zenodo.3460257)

- group based authorization (wlcg.groups)
- capability based authorization (scope)

use cases:

1) identity token with groups
2) access token with groups
3) access token with authorization scopes

SCITOKENS
scitokens.org

registering your OIDC app

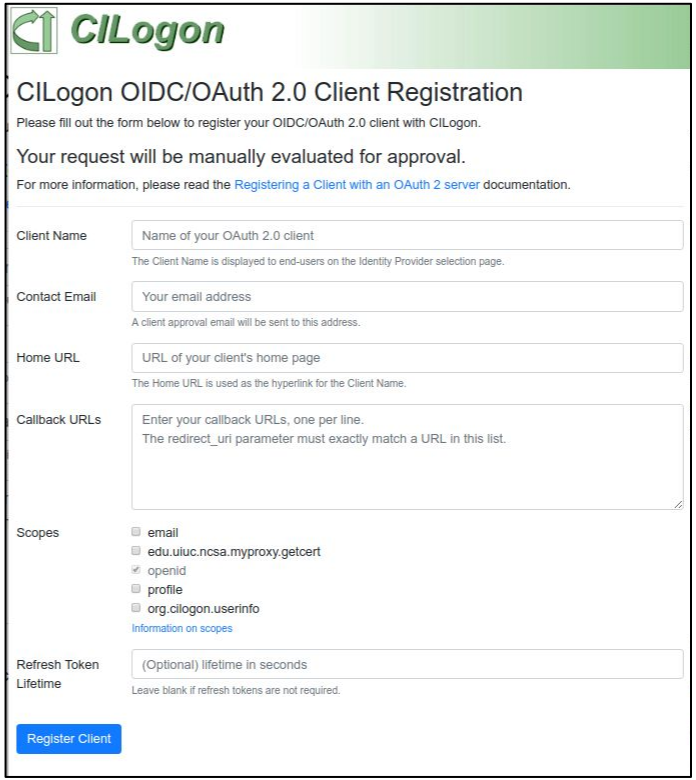
submit request at
https://cilogon.org/oauth2/register

including app details

save client_id and client_secret

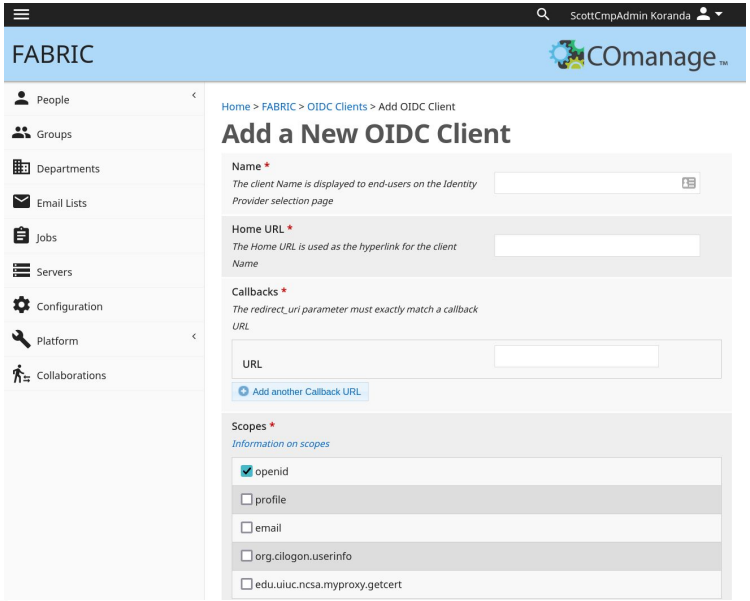
wait for notification
by help@cilogon.org

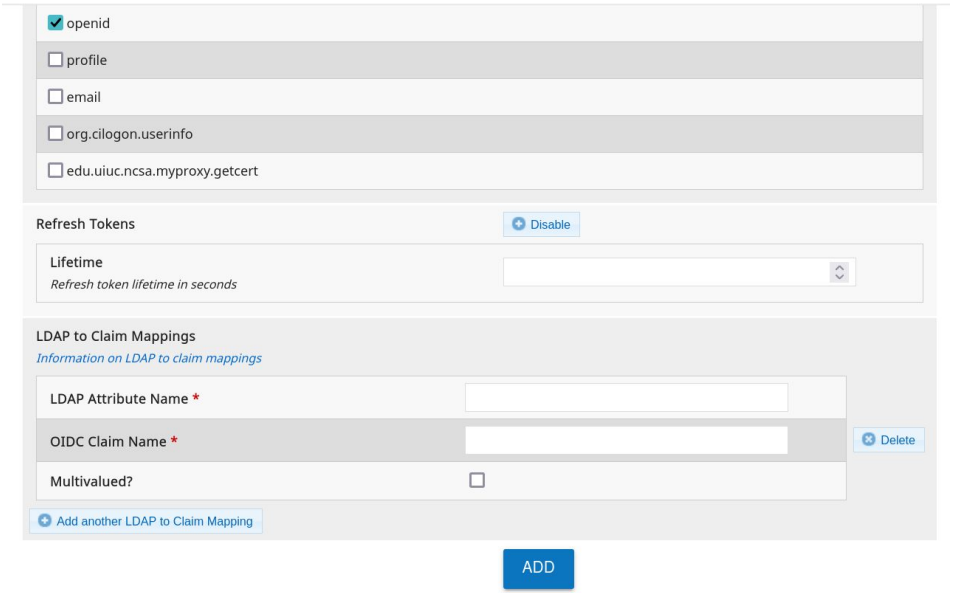
see docs:
http://www.cilogon.org/oidc



managing your OIDC apps

subscribers manage apps using COmanage





OAuth APIs for managing apps

subscribers can also manage OIDC apps via standard APIs:

- RFC 7591 - OAuth 2.0 Dynamic Client Registration Protocol
- RFC 7592 - OAuth 2.0 Dynamic Client Registration Management Protocol

examples of CILogon-enabled sites

Apache Airavata Test Drive, Ask.CI, ATLAS Connect, Australian BioCommons,
BNL Quantum Astrometry, Brainlife.io, CADRE, CERN PanDA, Chem Compute,
ClassTranscribe, CloudBank, Clowder, CMS Connect, Connect.ci, Custos,
CyberGISX, CyVerse, DataCite, DataONE, Duke CI Connect, Einstein Toolkit,
FABRIC, Fermilab, Flywheel, GeoChemSim, Globus, GW-Astronomy, HubICL,
ImPACT, LIGO, LROSE, LS-CAT, LSST, Mass Open Cloud,
MIT Engaging OnDemand, MSU HPCC OnDemand, MyGeoHub, NEON,
NIH ClinOmics, NIH KnowEnG, Ocean Observatories Initiative,
Open Science Chain, OSC OnDemand, OSG Connect,
Pacific Research Platform, QUBES, SciGaP, SCiMMA, SEAGrid, SeedMeLab,
SimVascular, Social Media Macroscope,
UCLA JupyterHub, Vanderbilt JupyterHub, and XSEDE

science gateways

enable web-based computational experiments and data management

CILogon-enabled hosted gateways:

Science Gateway Platform as a Service

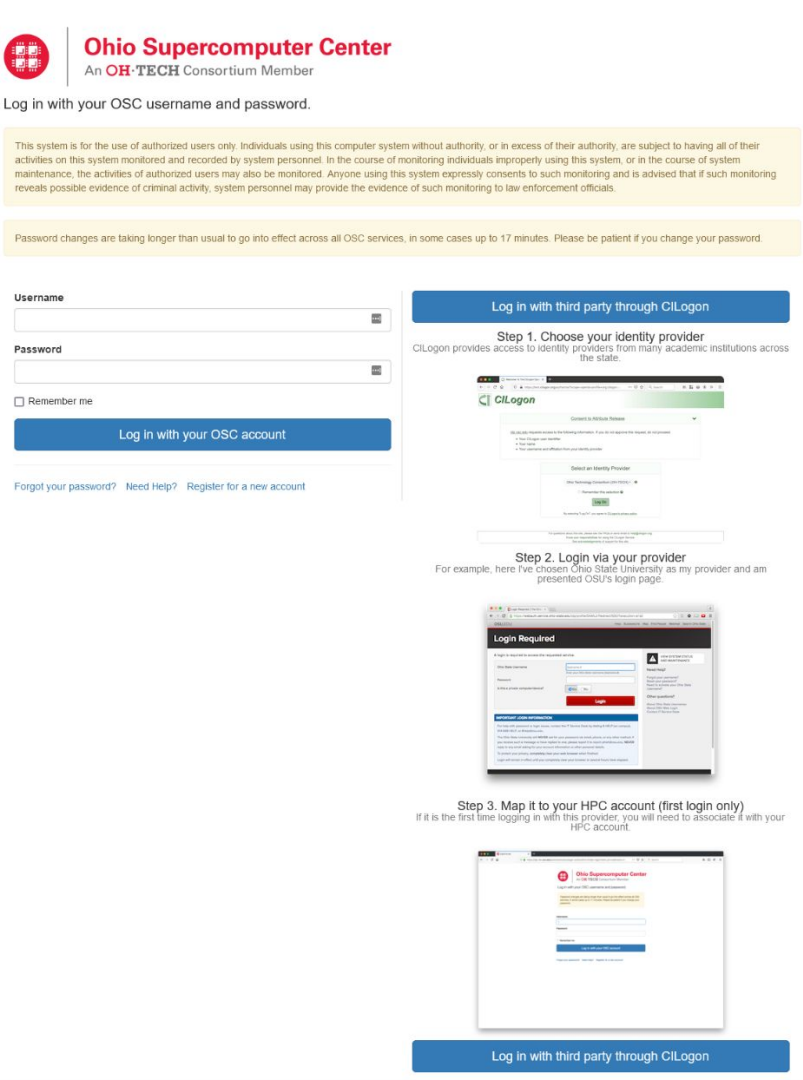
CUSTOS

OPEN OnDemand

Supercomputing. Seamlessly. Open, Interactive HPC Via the Web

- Support for Apache HTTP authentication modules including ADFS, CAS, OIDC, Shibboleth, Keycloak
- CILogon support via Keycloak
- Mapping federated identities to local accounts
- https://openondemand.org/
- https://osc.github.io/ood-documentation/latest/authentication

CILogon



Globus

campus authentication to your Globus Data Transfer Node

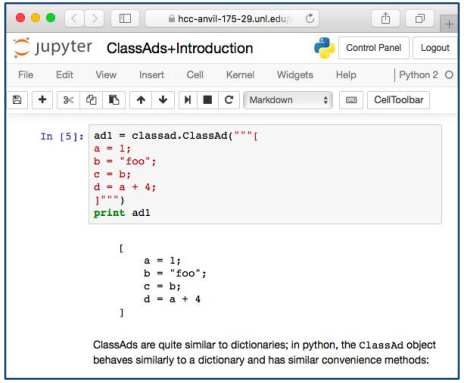
campus identities for Globus Auth

JupyterHub

notebooks support authoring/sharing of code, math, text, and multimedia

federated authentication using CILogon

one IdP or many



https://jupyterhub.readthedocs.io/en/latest/reference/authenticators.html
https://github.com/jupyterhub/oauthenticator
https://zero-to-jupyterhub.readthedocs.io/en/latest/authentication.html

Kubernetes

using Kubernetes native OIDC support

public clients, refresh tokens, API access

https://kubernetes.io/docs/reference/access-authn-authz/

demonstrated by PRP@UCSD

https://ucsd-prp.gitlab.io/userdocs/start/get-access/

CILogon

START TUTORIAL RUNNING STORAGE DEVELOPMENT BACK TO NAUTILUS BACK TO PRP

Get access
Quick Start
Policies
Available Resources
FAQ
Contact

Get access

To get an account on Pacific Research Platform kubernetes portal

1. To get access to the PRP Nautilus cluster, do the following
   - Point your browser to the PRP Nautilus portal
   - On the portal page click on "Login" button at the top right corner

   - You will be redirected to the "CILogon" page:

   - On this page, **select an Identity Provider** from the menu and **Click "Log On"** button to use your existing credentials for the chosen provider to sign in. The provider is one of :
   (1) If your institution is using CILogon as a federated certification authority it will be in the menu, select the name of your institution and use either a personal account or an institutional G-suite account. This is usually your institutional account name (email) and a password associated with it.
   (2) If your institution is not using CILogon, you can select "Google"
2. After a successful authentication you will login on the portal. On first login you become a **guest** and your account will need to be validated by the **admin users**. Any admin user can validate your guest account, promote you to **user** and add your account to their **namespace**. You need to be assigned to at least one namespace (usually a group project but can be your new namespace).
3. To notify admin users, use contact page to request that your account be upgraded from **guest** to **user**, and that you be added to a namespace (existing for a project or new one). To get access to a namespace, please contact its owner (usually email).
4. Once you are granted the **user** role in the cluster and are added to the namespace, you will get access to all namespace resources.
5. If you're starting a new project and would like to have your own namespace, either for yourself or for your group, you can request to be promoted to the **admin**. This will give you permission to create any number of namespaces and invite other users to your namespace(s). Please note, you'll be the one responsible for all activity happening in your namespaces.
6. Follow quick start page to start using kubernetes.

PRP is supported by its members institutions and the United States National Science Foundation through the NSF awards CNS-1456638, CNS-1730158, ACI-1540112, ACI-1541349, and OAC-1826967. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

© PACIFIC RESEARCH PLATFORM | DESIGN: PRP DESIGN TEAM

“Managed Services to Simplify Cloud Access for Computer Science Research and Education”

University of California, San Diego (UCSD)'s San Diego Supercomputer Center (SDSC) and Information Technology Services (ITS) Division
University of Washington (UW)'s eScience Institute
University of California, Berkeley (UCB)'s Division of Data Science

CloudBank

TRAINING ABOUT FAQ HELP LOG IN

Partners

HOME / ABOUT

CloudBank has engaged with these important public partners. Click on the company logo to learn more.

Strategic Blue

Beam

aws

Google Cloud

IBM Cloud

Microsoft Azure

CloudBank

TRAINING ABOUT FAQ HELP LOG IN

Log in

To **manage or access your CloudBank funds**, click the "Log in with *CILogon*" button using the instructions below. Login is currently limited to funded users. Contact help@cloudbank.org with any issues.

LOG IN WITH CILOGON

1. Click the "Log in with CILogon" button to visit a page for selecting login credentials.
2. Select an organization (Identity Provider) from the list to which you belong, and for which the email address matches your existing cloudbank.org account.
3. Click the "Log On" button to visit your organization's login page.
4. Login with your organization's credentials and you will be redirected back to cloudbank.org.

Consent to Attribute Release

CloudBank requests access to the following information. If you do not approve this request, do not proceed.

- Your CILogon user identifier
- Your name
- Your email address
- Your username and affiliation from your identity provider

Select an Identity Provider

University of Illinois at Urbana-Champaign

Remember this selection

Log On

By selecting "Log On", you agree to CILogon's privacy policy.

CloudBank

DASHBOARD TRAINING ABOUT FAQ HELP LOG OUT

Dashboard

Manage CloudBank Funds

View and manage your CloudBank funds and grant access to associated billing accounts (IAM).

Access CloudBank Billing Accounts

View all of your cloud billing accounts and current spend. Access public cloud web portals to manage cloud services.

Monitor & Optimize Your Usage

Access Nutanix Beam to monitor usage for each of accounts and view recommendations to optimize your usage.

CloudBank

DASHBOARD TRAINING ABOUT FAQ HELP LOG OUT

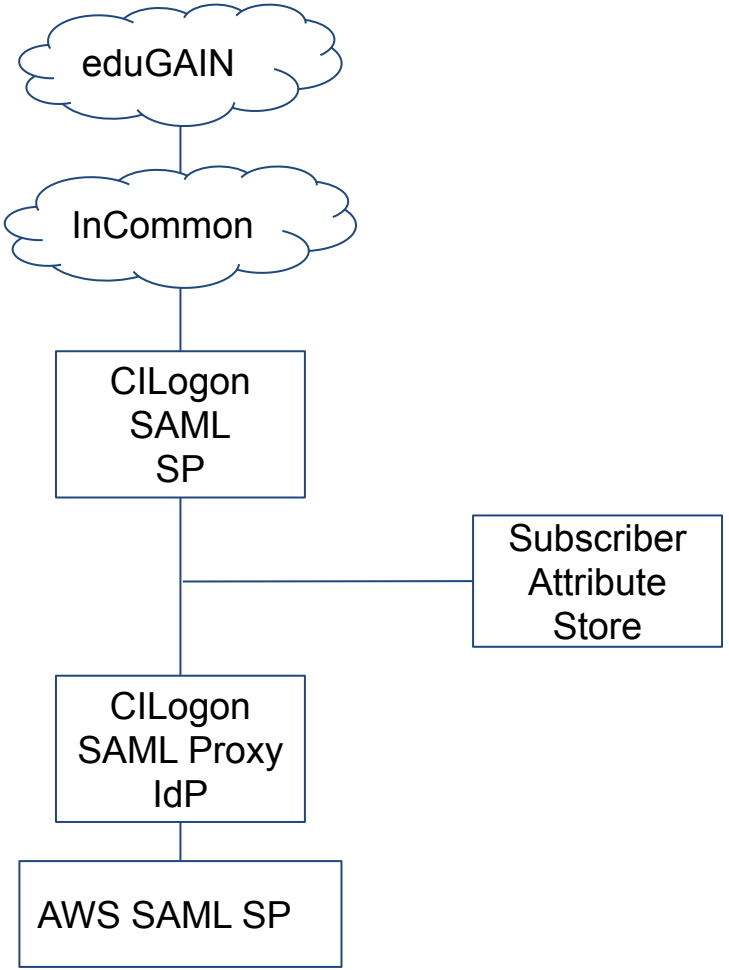
Billing Account Access

HOME / DASHBOARD

You have access to the following *billing account*s. A billing account can be dedicated or shared with multiple people. If you are in a shared billing account, please note that we can only track usage at the tag and service level so consult your billing account manager for assistance if you need to track usage at a finer granularity.

BILLING ACCOUNT ID	CLOUD USERNAME	INITIAL PRIVILEGES GRANTED	PUBLIC CLOUD	PUBLIC CLOUD WEB CONSOLE LOGIN	FUND	AWARD AMOUNT	BALANCE
713660817510	skoranda	Login	Amazon Web Services	login	Test Fund 1	$51.00 *	$41.39 (81%) *
test-2-1268	skoranda	Login (viewer)	Google Cloud Platform	login	Test Fund 2	$100.00 *	$31.58 (32%) *

* No specific limit specified on this *billing account*, value is inherited from *fund*.


eduGAIN
InCommon
CILogon
SAML
SP
Subscriber
Attribute
Store
CILogon
SAML Proxy
IdP
AWS SAML SP

Australian BioCommons

"To actively support life science research communities with community scale digital infrastructure developed and maintained in concert with international peer infrastructures."

Target ~30,000 life science researchers in AU

AUSTRALIAN
ACCESS FEDERATION

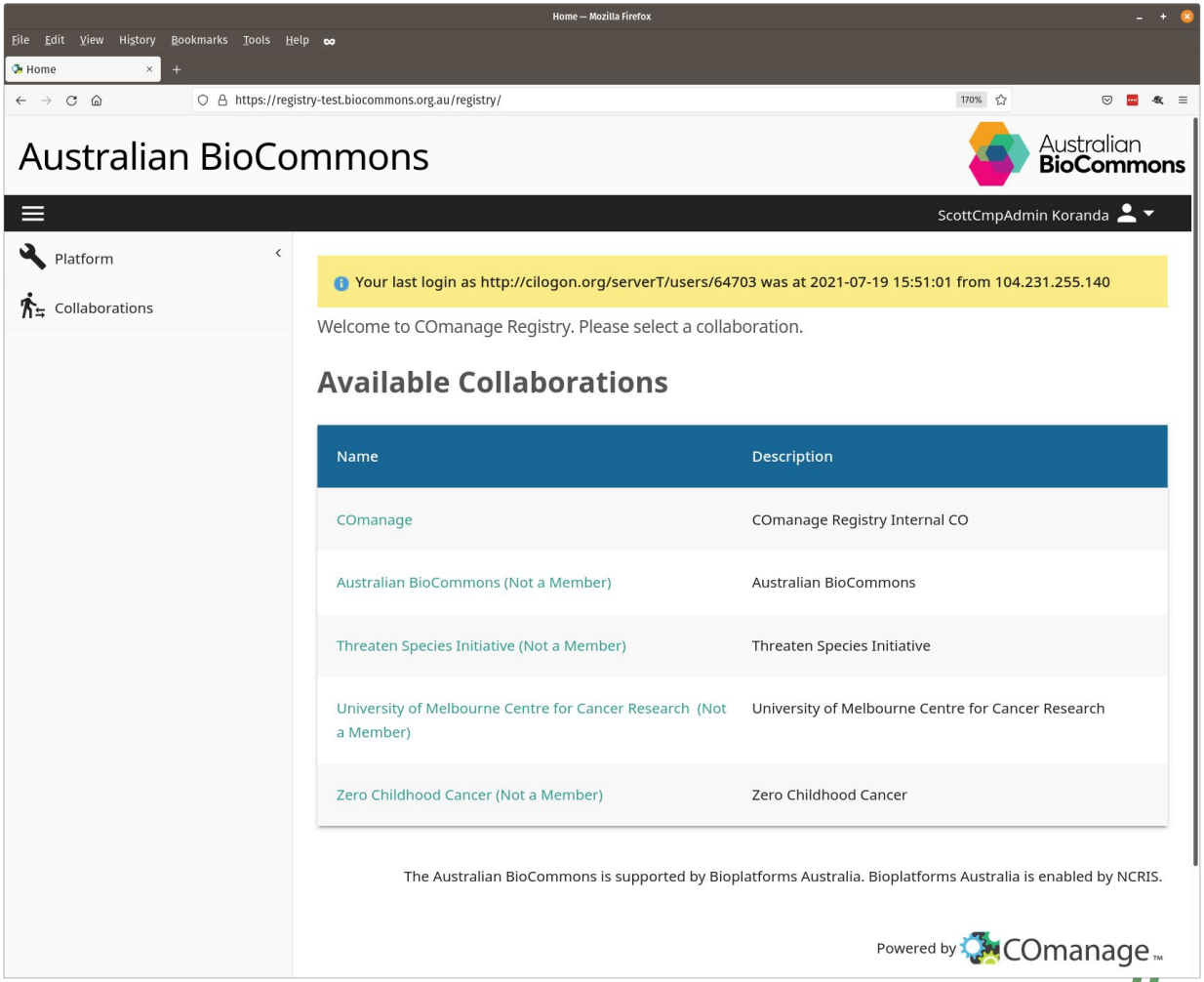
"Established in 2009, the Australian Access Federation (AAF) is Australia's identity federation and part of a global network of over 61 federations around the world."

Initial Collaboration Target

University of Melbourne Centre for Cancer Research (UMCCR)
"Driving innovation and implementation for clinical impact in cancer care"

Zero Childhood Cancer Program (ZERO)

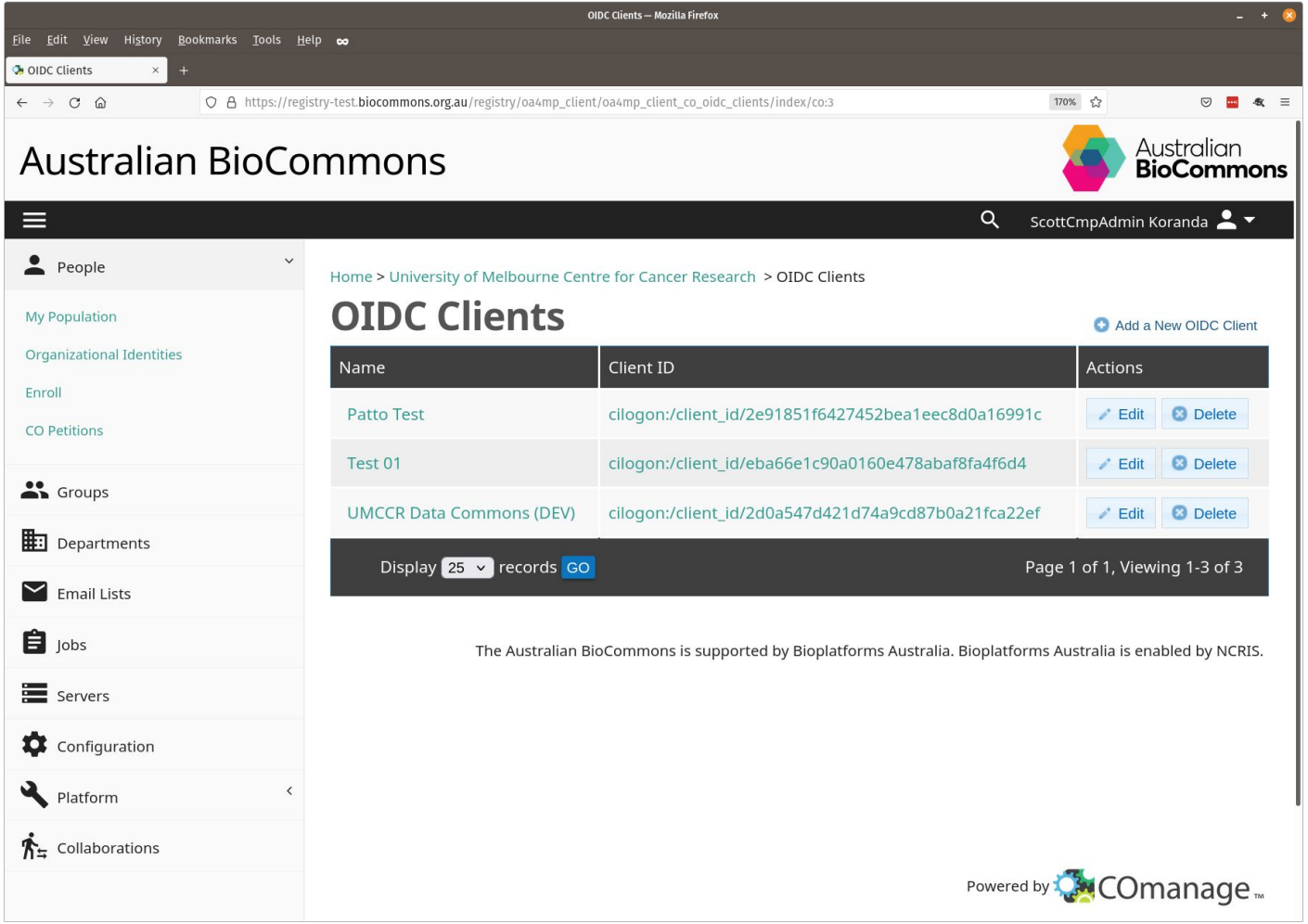
"Australia's first-ever personalised medicine program for children and young people with high-risk cancer"


Home — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Home
https://registry-test.biocommons.org.au/registry/
170%
Australian BioCommons
Australian BioCommons
ScottCmpAdmin Koranda
Platform
Collaborations
Your last login as http://cilogon.org/serverT/users/64703 was at 2021-07-19 15:51:01 from 104.231.255.140
Welcome to COmanage Registry. Please select a collaboration.
Available Collaborations
Name
Description
COmanage
COmanage Registry Internal CO
Australian BioCommons (Not a Member)
Australian BioCommons
Threaten Species Initiative (Not a Member)
Threaten Species Initiative
University of Melbourne Centre for Cancer Research (Not a Member)
University of Melbourne Centre for Cancer Research
Zero Childhood Cancer (Not a Member)
Zero Childhood Cancer
The Australian BioCommons is supported by Bioplatforms Australia. Bioplatforms Australia is enabled by NCRIS.
Powered by COmanage™

GEN3 DATA COMMONS

Center for Translational Data Science,
University of Chicago

“Gen3 Data Commons are cyberinfrastructure that co-locates data analysis, exploration and visualization tools with data management services for import and export of structured information like clinical, phenotypic, or biospecimen data, and data objects, like genomics data files or medical images.”


OIDC Clients — Mozilla Firefox
File Edit View History Bookmarks Tools Help
OIDC Clients
https://registry-test.biocommons.org.au/registry/oa4mp_client/oa4mp_client_co_oidc_clients/index/co:3
170%
Australian BioCommons
Australian BioCommons
ScottCmpAdmin Koranda
People
My Population
Organizational Identities
Enroll
CO Petitions
Groups
Departments
Email Lists
Jobs
Servers
Configuration
Platform
Collaborations
Home > University of Melbourne Centre for Cancer Research > OIDC Clients
OIDC Clients
Add a New OIDC Client
Name
Client ID
Actions
Patto Test
cilogon:/client_id/2e91851f6427452bea1eec8d0a16991c
Edit
Delete
Test 01
cilogon:/client_id/eba66e1c90a0160e478abaf8fa4f6d4
Edit
Delete
UMCCR Data Commons (DEV)
cilogon:/client_id/2d0a547d421d74a9cd87b0a21fca22ef
Edit
Delete
Display 25 records GO
Page 1 of 1, Viewing 1-3 of 3
The Australian BioCommons is supported by Bioplatforms Australia. Bioplatforms Australia is enabled by NCRIS.
Powered by COmanage™

uc-cdis / fence

Watch 33 | Unstar 23 | Fork 34

Code | Pull requests 55 | Actions | Security | Insights

First commit of CILogon authentication #896

Edit | Open with

Merged **paulineribeyre** merged 3 commits into `uc-cdis:master` from `cilogon:feat/cilogon` on Apr 21

Conversation 7 | Commits 3 | Checks 5 | Files changed 9 | +124 −3

skoranda commented on Apr 8 • edited by paulineribeyre | Contributor

First commit of CILogon authentication. CILogon provides a standards-compliant OpenID Connect (OAuth 2.0) interface to federated authentication including InCommon, the Australian Access Federation (AAF), and eduGAIN. CILogon OpenID Connect (OIDC) client registration is available to researchers and scholars at https://cilogon.org/oauth2/register

New Features

Add CILogon as an authentication option. CILogon provides a standards-compliant OpenID Connect (OAuth 2.0) interface to federated authentication including InCommon, the Australian Access Federation (AAF), and eduGAIN. CILogon OpenID Connect (OIDC) client registration is available to researchers and scholars at https://cilogon.org/oauth2/register

Reviewers

 **williamhaley** ✓

 **paulineribeyre** ✓

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Notifications Customize

Global Authz Interoperability

Global Alliance
for Genomics & Health

Collaborate. Innovate. Accelerate.

GA4GH Passports and the Authorization and Authentication Infrastructure

GA4GH AAI
OpenID Connect Profile

“In particular, this specification introduces a JSON Web Token (JWT) syntax for an access token to enable an OIDC provider (called a Broker) to allow a downstream access token consumer (called a Claim Clearinghouse) to locate the Broker’s /userinfo endpoint as a means to fetch GA4GH Claims. This specification is suggested to be used together with others that specify the syntax and semantics of the GA4GH Claims exchanged.”

CILogon Demo Success Page. — Mozilla Firefox

File Edit View History Bookmarks Tools Help

CILogon Demo Success

https://demo0.cilogon.org/cilogon2/ready?code=NB2HI4DTHIXS65DFON2C4Y3JNRXWO33OFZXXEZZPN5QXK5DIGIXTEMRZMY2TAZBSGFTDKNZWH

CILogon

Success!

- Show/Hide User Info


```
{
 "sub": "http://cilogon.org/serverT/users/27326098",
 "idp_name": "University of Illinois at Urbana-Champaign",
 "eppn": "skoranda@illinois.edu",
 "cert_subject_dn": "/DC=org/DC=cilogon/C=US/O=University of Illinois at Urbana-Champaign/CN=Scott Koranda T27326098",
 "eptid": "urn:mace:incommon:uiuc.edu!https://cilogon.org/shibboleth!3fsruagzH47Z8Q0fjwaXGRnFVR8=",
 "iss": "https://test.cilogon.org",
 "entitlement": "urn:mace:dir:entitlement:common-lib-terms",
 "given_name": "Scott",
 "acr": "urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport",
 "aud": "cilogon:test.cilogon.org/demo0",
 "idp": "urn:mace:incommon:uiuc.edu",
 "token_id": "https://test.cilogon.org/oauth2/idToken/7361b76653124b76098696b676fc41bf/1627044179747",
 "affiliation": "staff@illinois.edu;employee@illinois.edu;member@illinois.edu",
 "name": "Scott Koranda",
 "itrustuin": "659628827",
 "family_name": "Koranda",
 "ga4gh_passport_v1":  [
  "eyJ0eXAiOiJKV1QiLCJraWQiOiIyNDRCMjM1RjZCMjhFMzQxMDhEMTAxRUFDNzM2MkM0RSIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiJodHRwOi8vY2lsb2dvbi5vcmcvc2Vyd
  "eyJ0eXAiOiJKV1QiLCJraWQiOiIyNDRCMjM1RjZCMjhFMzQxMDhEMTAxRUFDNzM2MkM0RSIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiJodHRwOi8vY2lsb2dvbi5vcmcvc2Vyd
  "eyJ0eXAiOiJKV1QiLCJraWQiOiIyNDRCMjM1RjZCMjhFMzQxMDhEMTAxRUFDNzM2MkM0RSIsImFsZyI6IlJTMjU2In0.eyJzdWIiOiJodHRwOi8vY2lsb2dvbi5vcmcvc2Vyd
 ],
 "email": "skoranda@illinois.edu",
 "cid": "cilogon:test.cilogon.org/demo0"
}
```


- Show/Hide Access Token
- Show/Hide ID Token
- Show/Hide certificate subject

https://demo0.cilogon.org/

Thanks!

contact:

help@cilogon.org

extra slides

our vision

enable logon to scientific cyberinfrastructure (CI)

seamless IAM for academic research collaborations

use campus identity (eduGAIN/InCommon/Shibboleth)

manage onboarding/offboarding/attributes/groups/roles in one place (COmanage)

integrate with a variety of research apps
(OIDC, OAuth, JWT, SAML, LDAP, X.509, SSH)

our vision

enable logon to scientific cyberinfrastructure (CI)

seamless IAM for academic research collaborations

use campus identity (eduGAIN/InCommon/Shibboleth)

manage onboarding/offboarding/attributes/groups/roles in one place (COmanage, Grouper)

integrate with a variety of research apps
(OIDC, OAuth, JWT, SAML, LDAP, X.509, SSH)

via a non-profit, open source, reliable, sustainable hosted IAM service

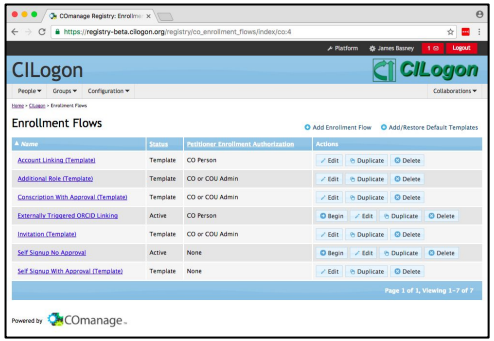
examples

grid computing

science gateways

jupyter notebooks

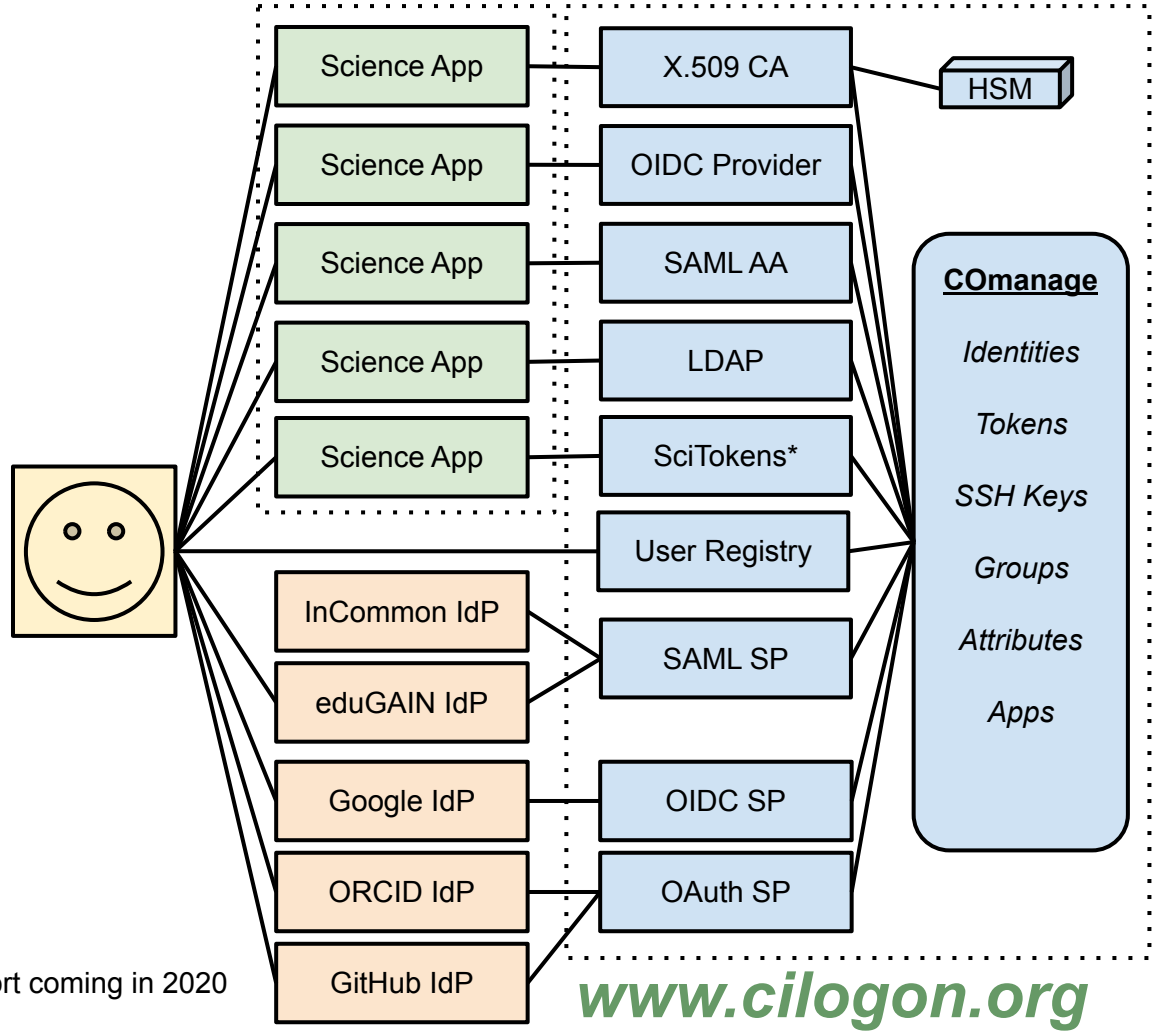
campus HPC clusters



federated identity management

and

collaborative organization management



CILogon

* SciTokens support coming in 2020

www.cilogon.org

building blocks

InCommon Federation:

single sign-on for US R&E

eduGAIN:

global interfederation

REFEDS:

international standards for R&E federations

InCommon Trusted Access Platform:

open source IAM software

InCommon Trusted Access Platform

Shibboleth: federated single sign-on

COmanage: collaborative organization management

Grouper: enterprise group and access management (including point-in-time auditing)

Midpoint: provisioning engine

https://www.incommon.org/trusted-access/

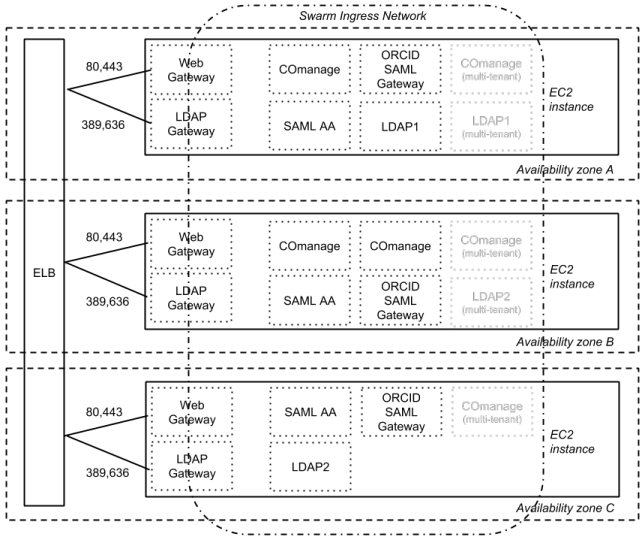
deployed to AWS

benefits of Net+ AWS

multiple availability zones

Docker containers in swarm mode

using R53 EC2 RDS ELB EFS



our baseline: REFEDS R&S

Attribute release continues to be the #1 stumbling block for new users.

We operate under the REFEDS R&S policy.

Does your campus support REFEDS R&S?

https://refeds.org/research-and-scholarship

https://cilogon.org/testidp/

REFEDS

security for global interfederation

We operate under the SIRTFI framework: Security Incident Response Trust Framework for Federated Identity

https://refeds.org/sirtfi

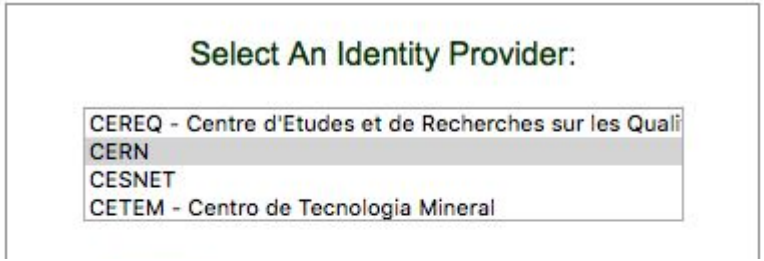
Supported by the NCSA Incident Response Team

https://security.ncsa.illinois.edu/

certificates for int'l science

CILogon CA policy update for int'l use approved in 2016 by Interoperable Global Trust Federation

Requiring R&S + Sirtfi



IGTF
AP | EU | TAG

managing project groups/roles

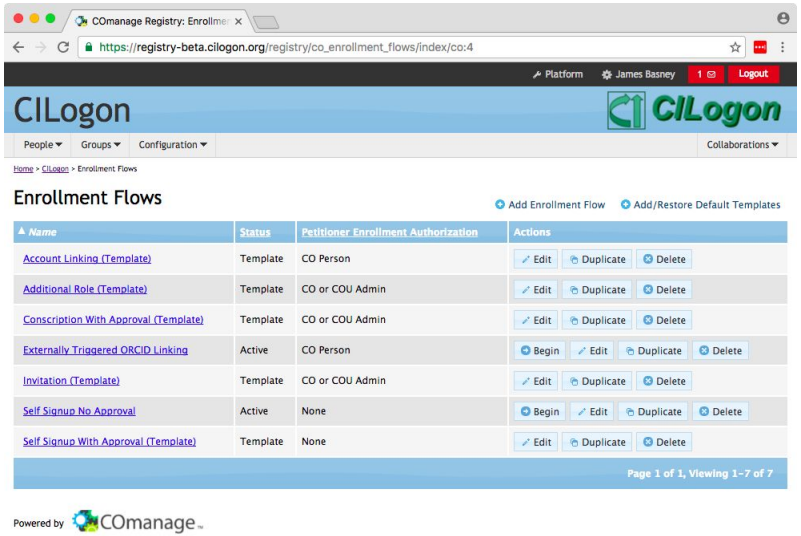
COmanage provides:

enrollment flows

expiration policies

self service permissions

pipelines



https://www.cilogon.org/comanage

collaboration management platform built for federated identity

Open Source

Internet2/InCommon

PHP

20+ deployments managing more than 50K federated identities

OpenID Connect (OIDC)

third gen OpenID (after OpenID 1.0/2.0)

- specifications: https://openid.net/connect/

authentication layer on top of OAuth 2.0 authorization framework (RFC 6749)

- adds new token type: ID Token
- adds new OAuth resource: UserInfo
- standard claims and scope values

MediaWiki

custom COmanage user identifier assignment for MediaWiki username

MediaWiki's OIDC extension for auth

- CILogon OIDC Provider sends custom MediaWiki username as sub claim

MediaWiki's OAuth extension for COmanage account provisioner

http://www.cilogon.org/mediawiki

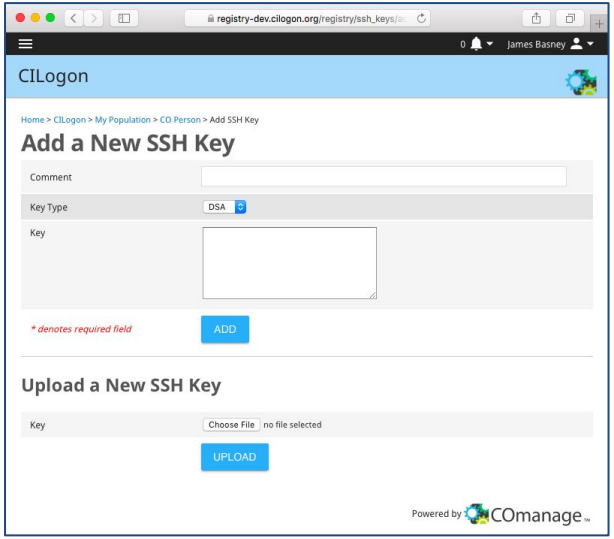
federated SSH keys

users register SSH public key during enrollment

associated with their federated identity

provisioned to LDAP

used by SSH server for authorization



https://serverfault.com/questions/653792/ssh-key-authentication-using-ldap

support for idphint specification

https://www.cilogon.org/oidc

https://aarc-project.eu/guidelines/aarc-g049/

AARC-G049 A specification for IdP hinting

This document defines a generic browser-based protocol for conveying – to services – hints about the IdPs or IdP-SP-proxies that should be used for authenticating the principal.

attribute-based authz example

eduPersonAffiliation: specifies the person's relationship(s) to the institution in broad categories

permissible values: faculty, student, staff, alum, member, affiliate, employee, library-walk-in

specification: https://refeds.org/eduperson

use cases:

- software licenses
- data access restrictions
- resource allocation limits

role-based authz example: AWS

COmanage assigns Roles to each Person

- via enrollment, approval workflows, expiration, etc.
- linked to federated identities of the Person

CILogon SAML Proxy asserts Roles to AWS at authentication time

- SAML proxy allows use of multiple identity providers

AWS IAM maps Roles to Permissions for access to AWS services

AWS Security Token Service (STS) provides temporary security credentials for CLI/API access

configuring your OIDC app

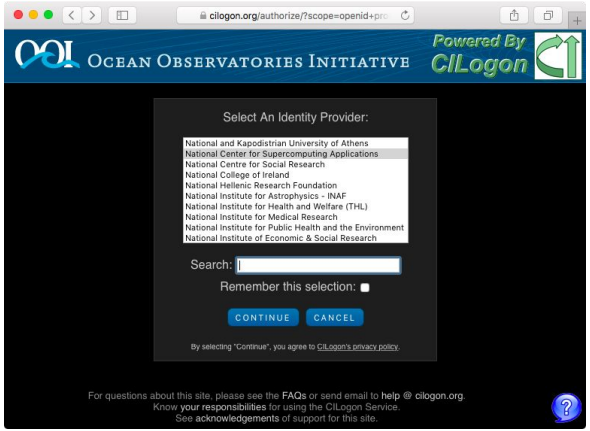
OIDC Discovery URL provides metadata

https://cilogon.org/.well-known/openid-configuration

contact help@cilogon.org to customize IdPs, claims, etc.

docs / examples:

http://www.cilogon.org/oidc



integration examples

science gateways
HPC clusters
Jupyter notebooks
wikis
mailing lists
Kubernetes

Globus
SSH
grid computing
AWS
G Suite
Auth0

seamless campus integration

bypass CILogon screens when accessing local campus research applications

- consent managed locally by campus
- always use campus IdP

an OpenID Connect proxy to your campus SAML IdP

- example: https://cybergateway.iu.edu/

bridging campus and VO IAM

passing campus and VO attributes to the application

- obtaining user consent via OIDC

manage VO attributes in COmanage

customize attributes/claims per app

- application-specific identifiers
- linking campus, researcher, and VO IDs
- driving authorization via group memberships

voPerson

an LDAP attribute schema (object class) with usage recommendations for VOs

voPersonApplicationUID	voPersonExternalID
voPersonAuthorName	voPersonID
voPersonCertificateDN	voPersonSoRID
voPersonCertificateIssuerDN	voPersonStatus

https://voperson.org/

Zoom Survey!
Thank you.

Next IAM Online: August 11, 2021, 2:00 p.m. ET

Go CAMPing

CAMP includes community presentations such as case studies, organizations' innovations in identity management, best practices, and other information that helps move the community forward.

2021 CAMP dates: October 4 - 8

Learn more at: https://incommon.org/academy/camp-meetings/2021-camp-week/