

CILogon

**Enabling Federated Identity and Access Management for
Scientific Collaborations**

Jim Basney <jbasney@ncsa.illinois.edu>
April 2022 MAGIC Meeting

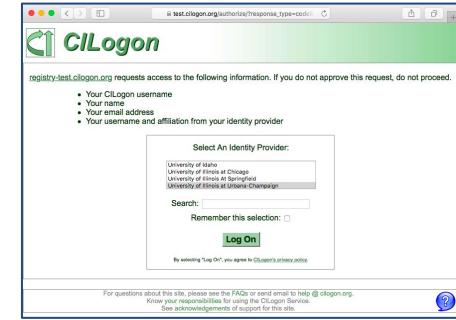


UNIVERSITY OF
ILLINOIS
URBANA-CHAMPAIGN



IAM for Research Collaborations

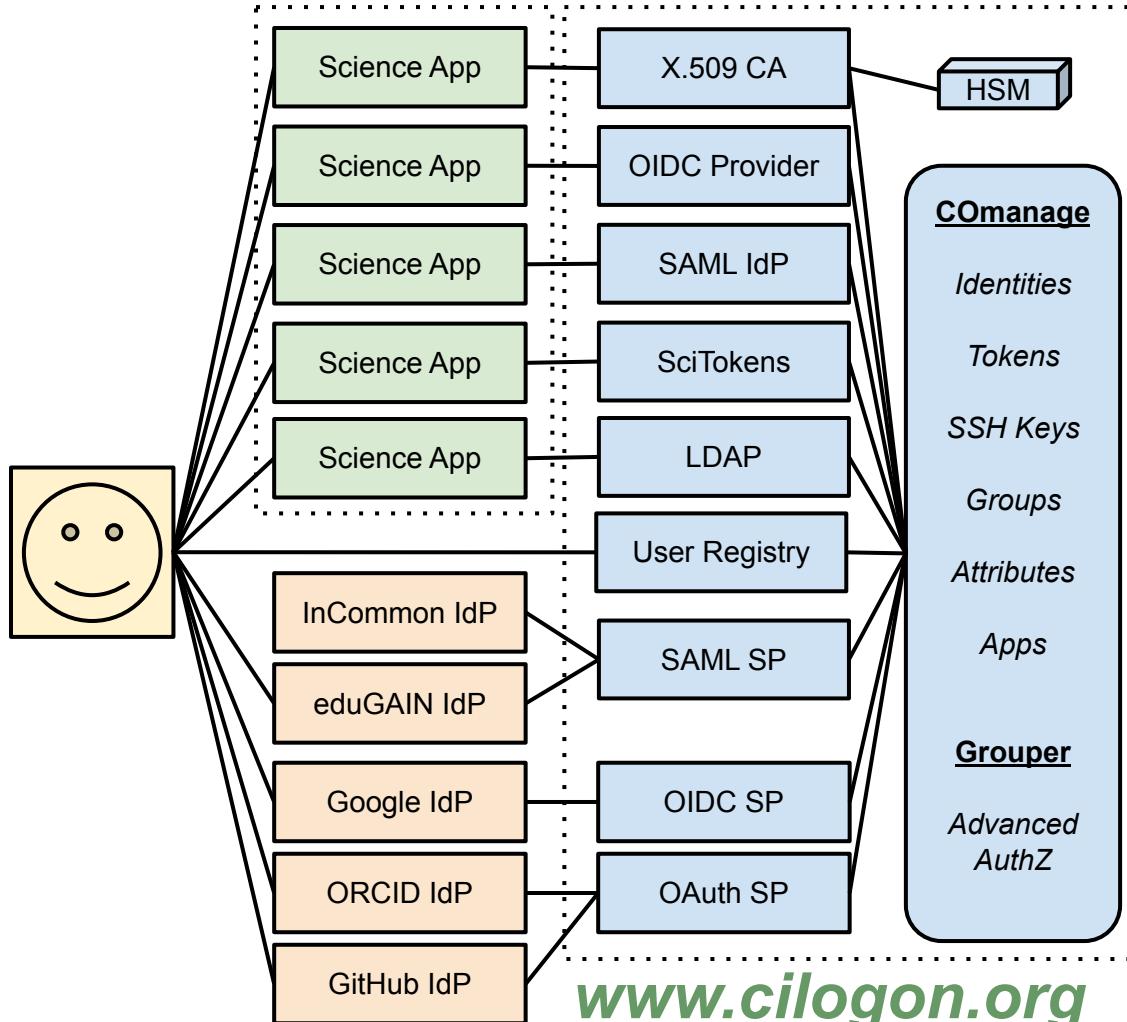
CILogon: 10+ year sustained effort to enable secure logon to scientific cyberinfrastructure (CI) for seamless identity and access management (IAM) using federated identities (SAML, OIDC, OAuth, JWT, X.509, LDAP, SSH, etc.) so researchers log on with their existing credentials from their home organization supporting 17,500+ active users from 450+ organizations around the world with onboarding/offboarding/attributes/groups/roles managed consistently across multiple applications



A screenshot of a web browser showing the CILogon 'Enrollment Flows' management interface. The URL is 'https://registry-beta.cilogon.org/registry/co_enrollment_flows/index/co:4'. The page title is 'CILogon'. It shows a table titled 'Enrollment Flows' with columns: 'Name', 'Status', 'Positioner Enrollment Authorization', and 'Actions'. The table lists several enrollment flow templates: 'Account Linking (Template)', 'Additional Role (Template)', 'Cancorrelation With Approval (Template)', 'Externally Triggered ORCID Linking', 'Instantiation (Template)', 'Self Signup No Approval', and 'Self Signup With Approval (Template)'. Each row has edit, duplicate, and delete buttons. At the bottom, it says 'Powered by COmanage.' and 'Page 1 of 1, Viewing 1-7 of 7'.

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



Extreme Science and Engineering
Discovery Environment

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.

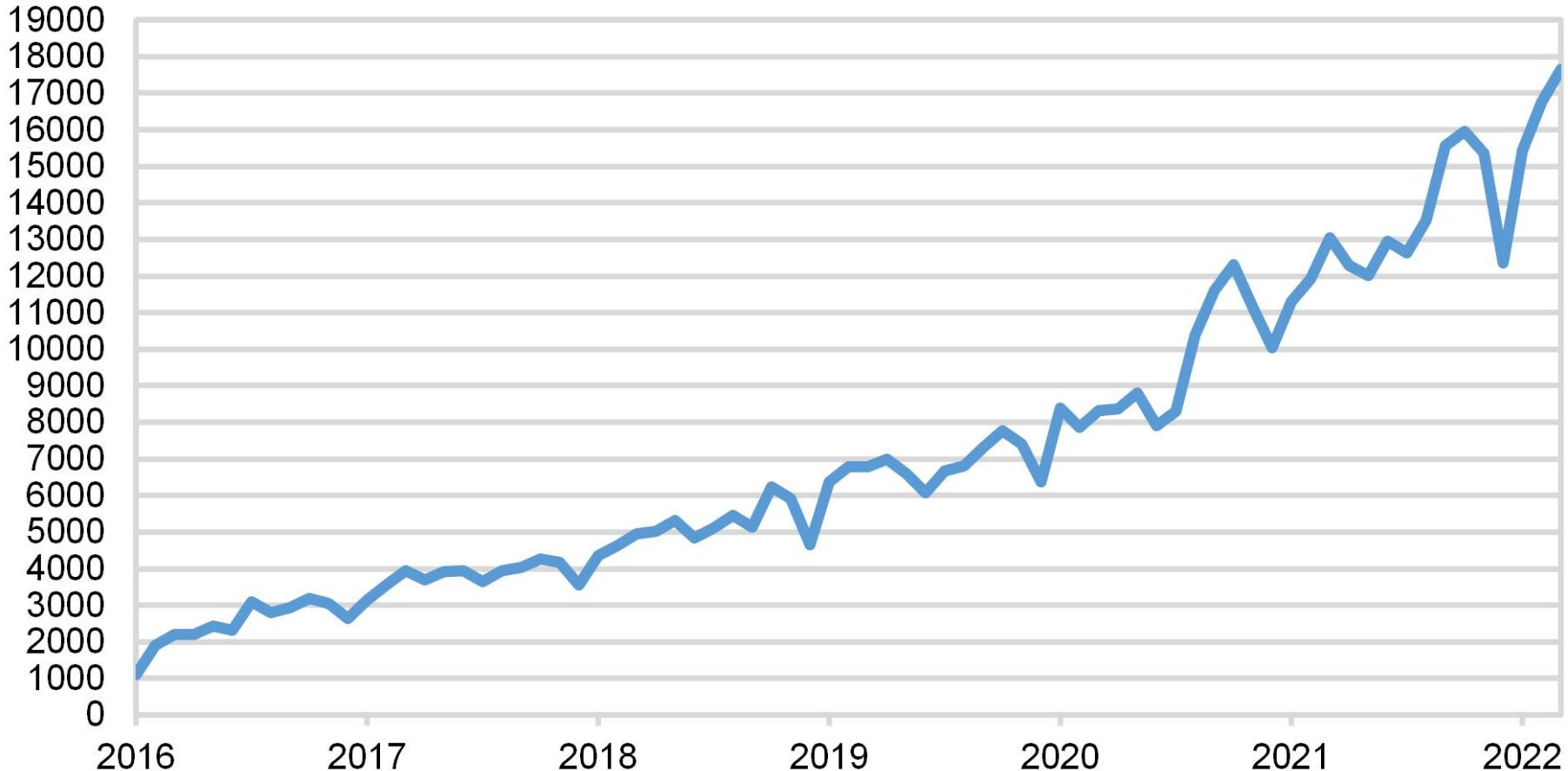
2017 COmanage support. AWS deployment.

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



Top 20 IdPs

(by # of unique active users in March 2022)

1315 Penn State	325 MIT
725 XSEDE	302 University of Chicago
720 University of Illinois at Urbana-Champaign	297 Washington University in St. Louis
665 Fermi National Accelerator Laboratory	264 NCSA
619 National Institutes of Health	255 Stanford University
514 LIGO Scientific Collaboration	251 Purdue University Main Campus
486 Northeastern University	240 University of Wisconsin-Madison
483 University of Michigan	216 Northwestern University
423 University of California-Los Angeles	208 University of California-San Diego
420 Michigan State University	189 Yale University

campus & researcher IDs

4,000+ identity providers available via eduGAIN

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

OAuth-based identity providers

ORCID GitHub Google Microsoft

supporting researcher mobility

supporting researchers w/o campus IdPs

managing 1000s of IdPs

SAML Metadata Query Protocol

<https://datatracker.ietf.org/doc/draft-young-md-query/>

<https://spaces.at.internet2.edu/display/MDQ>

monitor daily IdP changes

<https://groups.google.com/a/cilogon.org/g/idp-updates>

<https://cilogon.org/idplist/>

Want to see how adopting the MDQ metadata service affects your system's performance?

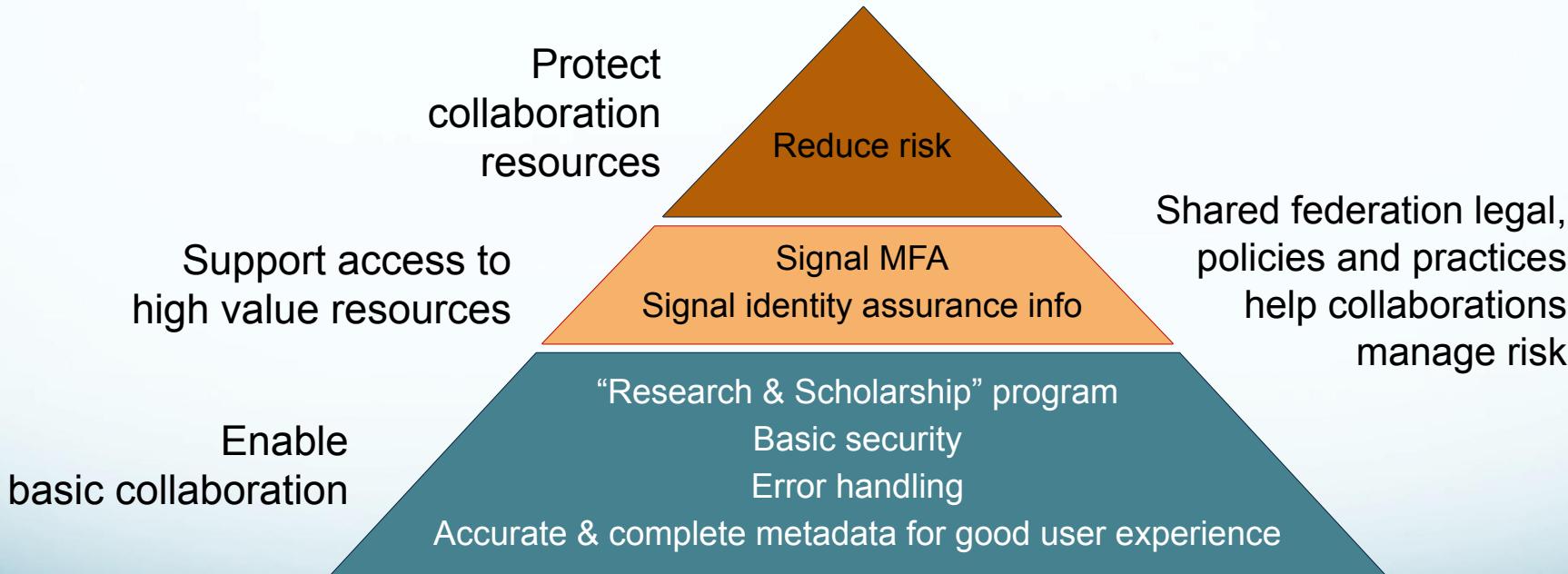
Here is an in-use memory graph at the moment a university switched to using MDQ in its production IdP servers:



Great results from a Service Provider:

"We were able to switch to using MDQ. The service restarts in 5 seconds now versus 15 minutes."

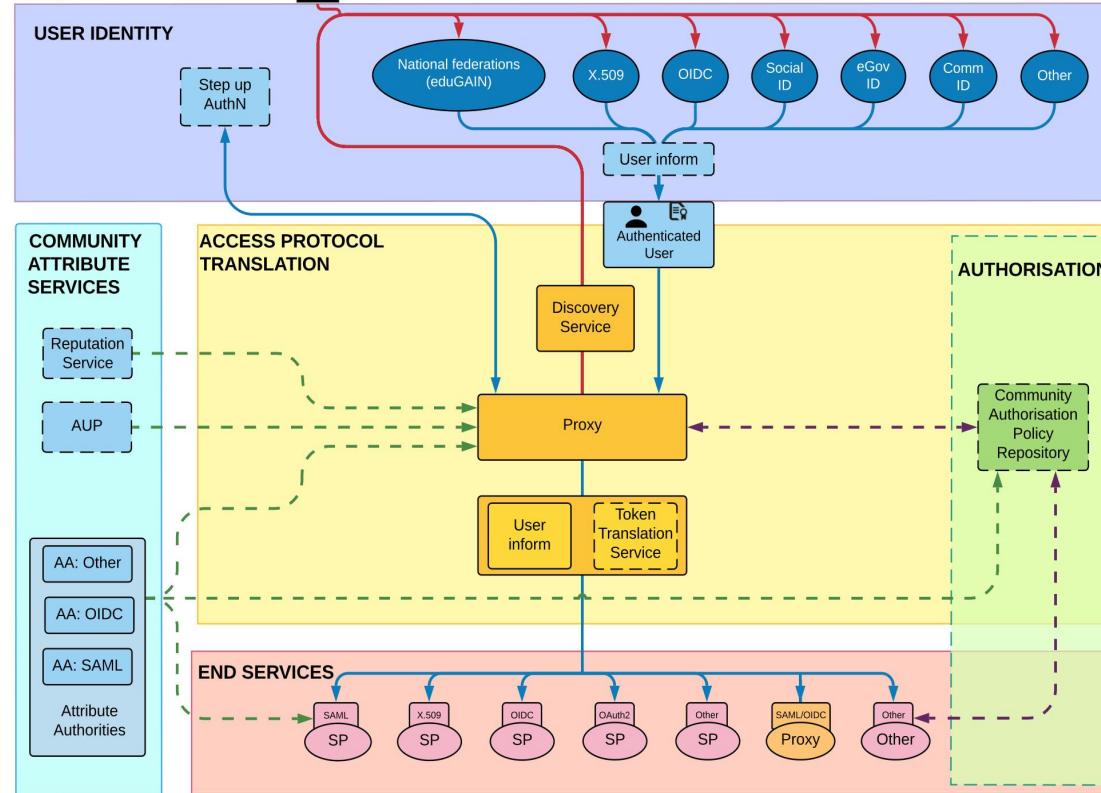
Federation support of research and scholarly communities



<https://www.incommon.org/federation/baseline/>



AARC Blueprint Architecture



<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

tokens for science

OpenID Connect (OIDC) ID Tokens (e.g., SCiMMA)
containing user attributes and group memberships
from the research community (via COmanage)
and from the researcher's home institution (via InCommon)



SciTokens (e.g., LIGO)
containing authorization scope values
determined by per client/subscriber policy



WLCG Tokens (e.g., Fermilab)
support for wlcg.groups and storage.*|compute.* scopes



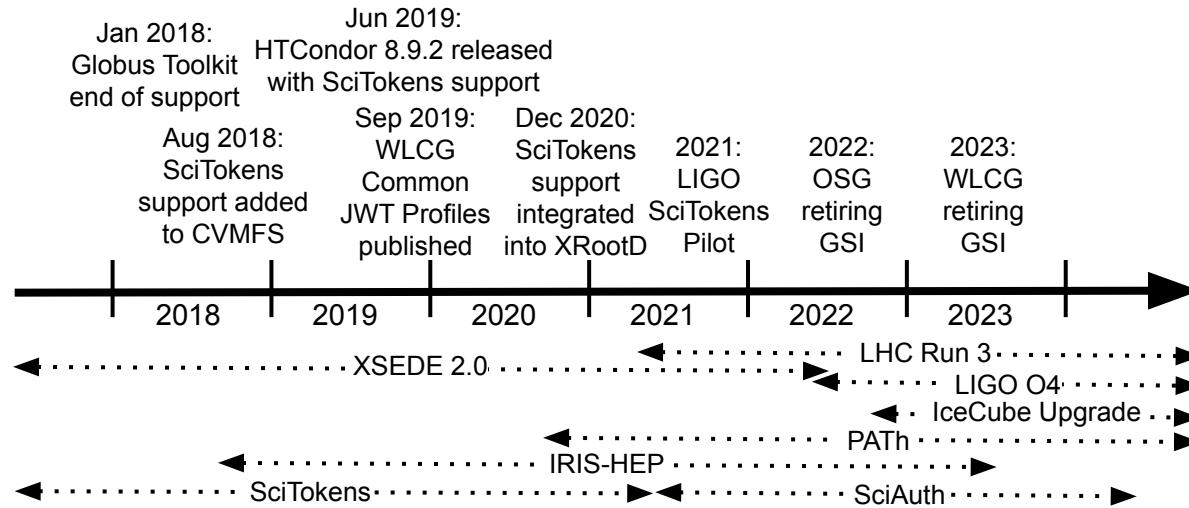
GA4GH Passports (e.g., Australian BioCommons)
support for AffiliationAndRole, AcceptedTermsAndPolicies, ResearcherStatus,
ControlledAccessGrants, and LinkedIdentities

token standards

- RFC 6749: OAuth 2.0 Authorization Framework
 - token request, consent, refresh
- RFC 7519: JSON Web Token (JWT)
 - self-describing tokens, distributed validation
- RFC 8414: OAuth 2.0 Authorization Server Metadata
 - token signing keys, policies, endpoint URLs
- RFC 8693: OAuth 2.0 Token Exchange
 - token delegation, drop privileges (reduce "scope")
- RFC 9068: JWT Profile for OAuth 2.0 Access Tokens
 - authorization claims using JWT "scope" and "aud"

<https://www.cilogon.org/jwt>

token transition timeline



<https://opensciencegrid.org/docs/security/tokens/overview/>

<https://sciauth.org/>

informed consent

The screenshot shows a web browser window with the following details:

- Address Bar:** cilogon.org/authorize/?nonce=6HBYAITAmIX
- Logos:** The Globus logo (a white 'g' inside a blue cloud-like shape) and the CILogon logo (the word "Powered By" above "CILogon" next to a green circular arrow icon).
- Text:** "Globus requests access to the following information. If you do not approve this request, do not proceed."
- List:** A bulleted list of requested information:
 - Your CILogon username
 - Your name
 - Your email address
 - Your username and affiliation from your identity provider
 - A certificate that allows "Globus" to act on your behalf
- Form:** A box containing:
 - Selected Identity Provider:** University of Illinois at Urbana-Champaign
 - Remember this selection:**
 - Log On** button
- Text:** "By selecting "Log On", you agree to CILogon's privacy policy."
- Footer:** "For questions about this site, please see the [FAQs](#) or send email to [help @ cilogon.org](mailto:help@cilogon.org). Know [your responsibilities](#) for using the CILogon Service. See [acknowledgements](#) of support for this site." A blue question mark icon is also present.

examples of CILogon-enabled sites

2i2c, 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, Duke CI Connect,
Einstein Toolkit, FABRIC, Fermilab, Flywheel, GeoChemSim, Globus,
GW-Astronomy, HubICL, HTCondor, 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



“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

<https://www.cloudbank.org/>

Partners

[HOME](#) / [ABOUT](#)

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



Beam



Google Cloud



IBM Cloud



Microsoft
Azure



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 

By selecting "Log On", you agree to [CILogon's privacy policy](#).

For questions about this site, please see the [FAQs](#) or send email to help@cielogon.org.

Know [your responsibilities](#) for using the CILogon Service.
See [acknowledgements](#) of support for this site.

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.

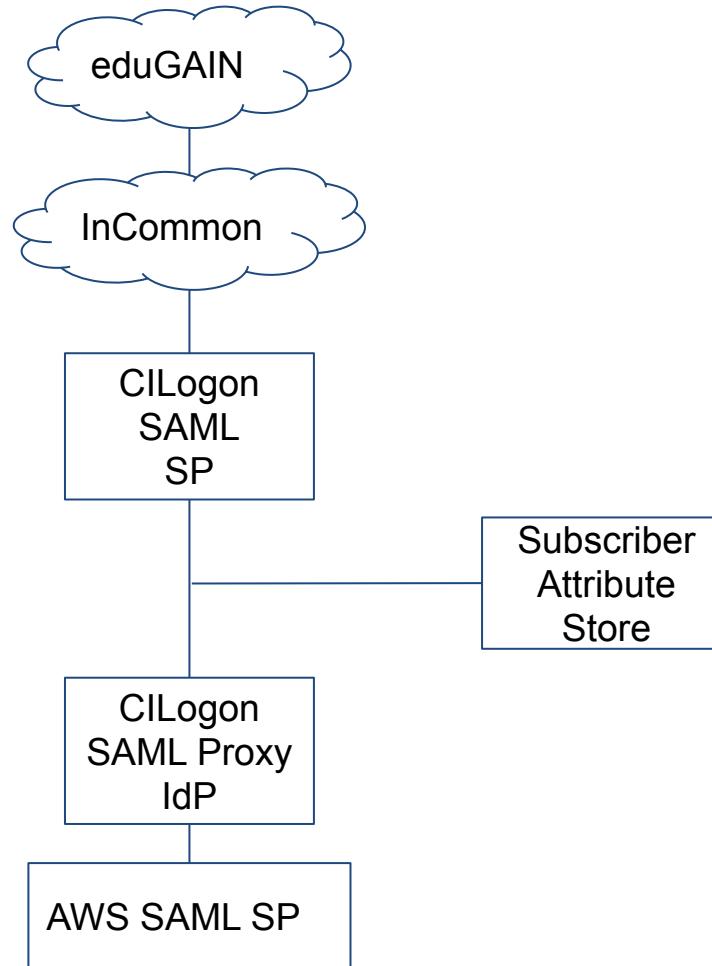
Billing Account Access

[HOME](#) / [DASHBOARD](#)

You have access to the following *billing accounts*. 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*.



Thanks!

contact:

help@cilogon.org

subscribe for updates:

<https://groups.google.com/a/cilogon.org/g/announce>

extra slides

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/>

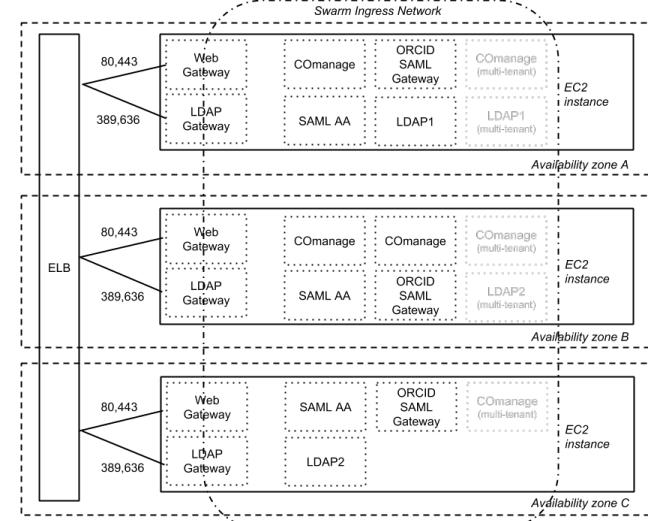
deployed to AWS

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/>



security for global interfederation

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

<https://refeds.org/sirtfi>

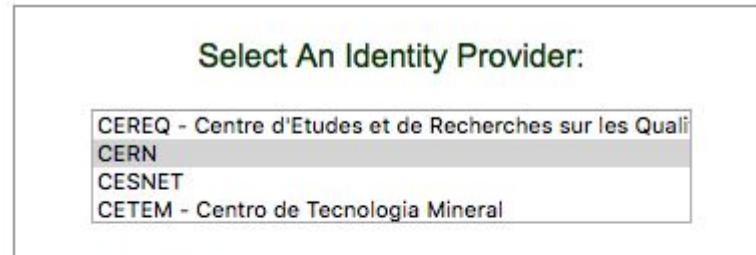
Supported by the NCSA Incident
Response Team

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



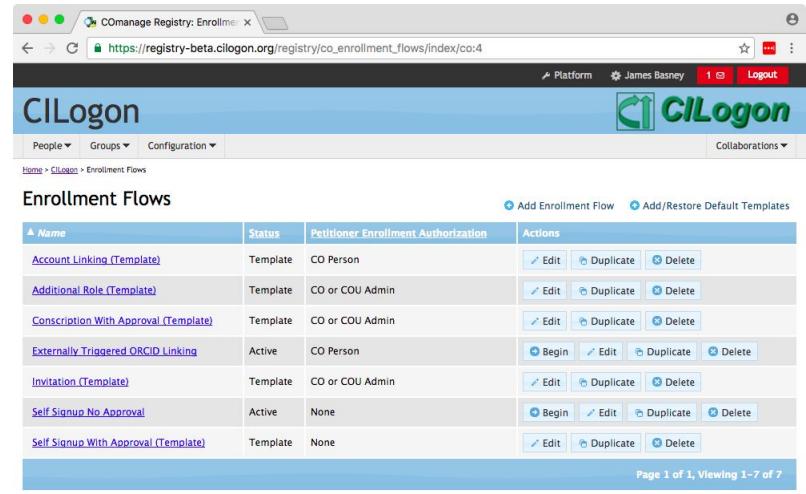
certificates for int'l science

CILogon CA policy update for int'l use approved in 2016 by Interoperable Global Trust Federation
Requiring R&S + Sirtfi



managing project groups/roles

COmanage provides:
enrollment flows
expiration policies
self service permissions
pipelines



The screenshot shows a web browser window for the COmanage Registry. The URL is https://registry-beta.cilogon.org/registry/co_enrollment_flows/index/co:4. The page title is "CILogon". The main content area is titled "Enrollment Flows". It displays a table with the following data:

Name	Status	Petitioner Enrollment Authorization	Actions
Account Linking (Template)	Template	CO Person	Edit Duplicate Delete
Additional Role (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Conscription With Approval (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Externally Triggered ORCID Linking	Active	CO Person	Begin Edit Duplicate Delete
Invitation (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Self Signup No Approval	Active	None	Begin Edit Duplicate Delete
Self Signup With Approval (Template)	Template	None	Edit Duplicate Delete

Page 1 of 1, Viewing 1–7 of 7

Powered by  Comanage

<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

science gateways

enable web-based computational experiments and data management

CILogon-enabled hosted gateways:

Science Gateway Platform as a Service



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>



Ohio Supercomputer Center

An OH-TECH Consortium Member

Log in with your OSC username and password.

This system is for the use of authorized users only. Individuals using this computer system without authority, or in excess of their authority, are subject to having all of their activities on this system monitored and recorded by system personnel. In the course of monitoring individuals improperly using this system, or in the course of system maintenance, the activities of authorized users may also be monitored. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Password changes are taking longer than usual to go into effect across all OSC services, in some cases up to 17 minutes. Please be patient if you change your password.

Username

Password

Remember me

Log in with your OSC account

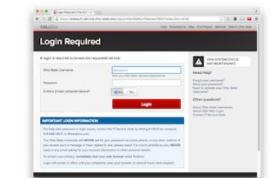
[Forgot your password?](#) [Need Help?](#) [Register for a new account](#)

Log in with third party through CILogon

Step 1. Choose your identity provider
CILogon provides access to identity providers from many academic institutions across the state.



Step 2. Login via your provider
For example, here I've chosen Ohio State University as my provider and am presented OSU's login page.



Step 3. Map it to your HPC account (first login only)
If it is the first time logging in with this provider, you will need to associate it with your HPC account.



Log in with third party through CILogon

Globus

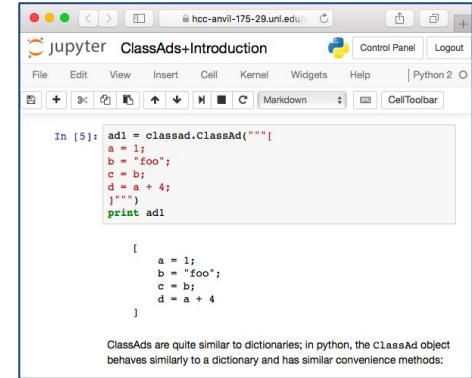
campus authentication to your
Globus Data Transfer Node

campus identities for Globus Auth



JupyterHub

notebooks support authoring/sharing of
code, math, text, and multimedia
federated authentication using CILogon
one IdP or many



A screenshot of a Jupyter Notebook interface. The title bar says "jupyter ClassAds+Introduction". The menu bar includes File, Edit, View, Insert, Cell, Kernel, Widgets, Help, and Python 2. The toolbar has icons for file operations like Open, Save, and Run. The code cell contains the following Python code:

```
In [5]: ad1 = classad.ClassAd("""  
a = 1;  
b = "foo";  
c = b;  
d = a + 4;  
""")  
print ad1
```

The output cell shows the result:

```
[  
a = 1;  
b = "foo";  
c = b;  
d = a + 4  
]
```

A note at the bottom right says: "ClassAds are quite similar to dictionaries; in python, the ClassAd object behaves similarly to a dictionary and has similar convenience methods."



<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/>



START TUTORIAL RUNNING STORAGE DEVELOPMENT BACK TO NAUTILUS BACK TO PRP

Get access Quick Start Policies Available Resources To get an account on Pacific Research Platform kubernetes portal FAQ Contact

Get access

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

PRP Kubernetes portal

This is the login page for the PRP Kubernetes cluster. Please enter your credentials to log in with your institution's identity provider.

You can also log in with your local account. Please click here to log in with your local account.

CILogon

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

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

Select An Identity Provider:

J.U. Tell University
AAT Virtual University
AAT Virtual University - Sign On Service
Aalto University

Search: Remember this selection:

Log On

By selecting "Log On", you agree to CILogon's terms and conditions.

• 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-1730155, ACI-1540012, ACI-1541549, 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.

MediaWiki



custom COmanage user identifier assignment for MediaWiki username

MediaWiki's OIDC extension for auth

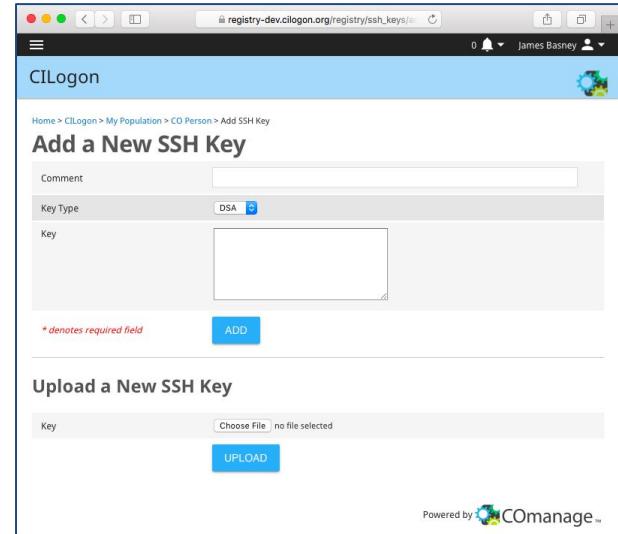
CILogon OIDC Provider sends custom MediaWiki username as sub claim

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

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>



CILogon

CILogon OIDC/OAuth 2.0 Client Registration

Please fill out the form below to register your OIDC/OAuth 2.0 client with CILogon.

Your request will be manually evaluated for approval.

For more information, please read the [Registering a Client with an OAuth 2 server](#) documentation.

Client Name	Name of your OAuth 2.0 client. The Client Name is displayed to end-users on the Identity Provider selection page.
Contact Email	Your email address. A client approval email will be sent to this address.
Home URL	URL of your client's home page The Home URL is used as the hyperlink for the Client Name.
Callback URLs	Enter your callback URLs, one per line. The redirect_uri parameter must exactly match a URL in this list.
Scopes	<input type="checkbox"/> email <input type="checkbox"/> edu.uiuc.ncsa.myproxy.getcert <input checked="" type="checkbox"/> openid <input type="checkbox"/> profile <input type="checkbox"/> org.cilogon.userinfo Information on scopes
Refresh Token Lifetime	(Optional) lifetime in seconds Leave blank if refresh tokens are not required.

[Register Client](#)

managing your OIDC apps

subscribers manage apps using COmanage

The screenshot shows the FABRIC interface with a sidebar containing 'People', 'Groups', 'Departments', 'Email Lists', 'Jobs', 'Servers', 'Configuration', 'Platform', and 'Collaborations'. The main area displays the 'Add a New OIDC Client' form. It includes fields for 'Name' (with a note about being displayed to end-users), 'Home URL' (with a note about being the hyperlink for the client), 'Callbacks' (with a note about matching the redirect_uri parameter), and 'Scopes' (checkboxes for openid, profile, email, org.cilogon.userinfo, and edu.uiuc.ncsa.myproxy.getcert). A 'Provider selection page' link is also present.

The screenshot shows the COmanage interface with a sidebar. The main area displays the 'OIDC Client Settings' form. It includes sections for 'Scopes' (checkboxes for openid, profile, email, org.cilogon.userinfo, and edu.uiuc.ncsa.myproxy.getcert), 'Refresh Tokens' (with a 'Lifetime' field and a 'Disable' button), and 'LDAP to Claim Mappings' (with fields for 'LDAP Attribute Name', 'OIDC Claim Name', and 'Multivalued?' checkbox). A blue 'ADD' button is located at the bottom right.

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

configuring your OIDC app

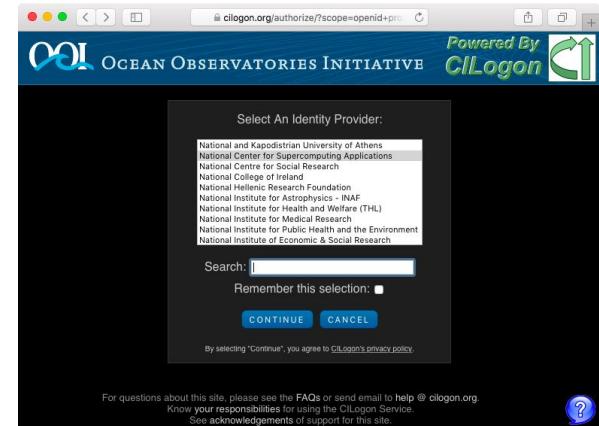
OIDC Discovery URL provides metadata

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

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

docs / examples:

<http://www.cilogon.org/oidc>



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/>



“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



“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% ScottCmpAdmin Koranda

Australian BioCommons

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.



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.”

Code

Pull requests 55

Actions

Security

Insights

First commit of CILogon authentication #896

Edit

Open with ▾



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

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



CILogon

www.cilogon.org

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.”

File Edit View History Bookmarks Tools Help ☰

CILogon Demo Success X +

https://demoo.cilogon.org/cilogon2/ready?code=N82H14DTHIXS65DFON2C4Y3JNRXWO33OFZXXEZZPN5QX5DIGITEMRZMY2TAZBSGFTDKNZWH... 170% ⌂ ⌃ ⌄ ⌅ ⌆ ⌇ ⌈ ⌉ ⌊ ⌋



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",  
    "epid": "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": [  
        "eyJ0eXAiOiJKV1QiLCJraWQiOiIyNDRCMjM1RjZCMjhFMzQxMDhEMTAXRUFDNzM2MkM0RSIsImFsZyI6IlJTMyU2In0.eyJzdWIi0iJodHRw0i8vY2lsb2dvbi5vcmcv2Vyd  
        "eyJ0eXAiOiJKV1QiLCJraWQiOiIyNDRCMjM1RjZCMjhFMzQxMDhEMTAXRUFDNzM2MkM0RSIsImFsZyI6IlJTMyU2In0.eyJzdWIi0iJodHRw0i8vY2lsb2dvbi5vcmcv2Vyd  
        "eyJ0eXAiOiJKV1QiLCJraWQiOiIyNDRCMjM1RjZCMjhFMzQxMDhEMTAXRUFDNzM2MkM0RSIsImFsZyI6IlJTMyU2In0.eyJzdWIi0iJodHRw0i8vY2lsb2dvbi5vcmcv2Vyd  
    ],  
    "email": "skoranda@illinois.edu",  
    "cid": "cilogon:test.cilogon.org/demo0"  
}
```

- [Show/Hide Access Token](#)
- [Show/Hide ID Token](#)
- [Show/Hide certificate subject](#)