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
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.
<table>
<thead>
<tr>
<th>Rank</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>National Institutes of Health</td>
</tr>
<tr>
<td>2</td>
<td>Fermi National Accelerator Laboratory</td>
</tr>
<tr>
<td>3</td>
<td>XSEDE</td>
</tr>
<tr>
<td>4</td>
<td>LIGO Scientific Collaboration</td>
</tr>
<tr>
<td>5</td>
<td>University of Michigan</td>
</tr>
<tr>
<td>6</td>
<td>University of Illinois Urbana-Champaign</td>
</tr>
<tr>
<td>7</td>
<td>Michigan State University</td>
</tr>
<tr>
<td>8</td>
<td>Penn State</td>
</tr>
<tr>
<td>9</td>
<td>Massachusetts Institute of Technology</td>
</tr>
<tr>
<td>10</td>
<td>University of Chicago</td>
</tr>
<tr>
<td>11</td>
<td>Purdue University Main Campus</td>
</tr>
<tr>
<td>12</td>
<td>Yale University</td>
</tr>
<tr>
<td>13</td>
<td>Stanford University</td>
</tr>
<tr>
<td>14</td>
<td>NCSA</td>
</tr>
<tr>
<td>15</td>
<td>University of California-Los Angeles</td>
</tr>
<tr>
<td>16</td>
<td>University of California-San Diego</td>
</tr>
<tr>
<td>17</td>
<td>Johns Hopkins</td>
</tr>
<tr>
<td>18</td>
<td>Northwestern University</td>
</tr>
<tr>
<td>19</td>
<td>Northeastern University</td>
</tr>
<tr>
<td>20</td>
<td>University of North Carolina Chapel Hill</td>
</tr>
</tbody>
</table>
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
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

science gateways

enable web-based computational experiments and data management

CILogon-enabled hosted gateways:

Science Gateway Platform as a Service
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
Globus

campus authentication to your Globus Data Transfer Node
campus identities for Globus Auth

Globus

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

https://github.com/jupyterhub/oauthenticator
Kubernetes

using Kubernetes native OIDC support for 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/
“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

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

![CIlogon logo](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 CloudBank 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 CloudBank's privacy policy.

For questions about this site, please see the FAQs or send email to help@cilogon.org.

Know your responsibilities for using the CloudBank Service.

See acknowledgments of support for this site.
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

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.

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

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

Welcome to COmanage Registry. Please select a collaboration.

Available Collaborations

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>COmanage</td>
<td>COmanage Registry Internal CO</td>
</tr>
<tr>
<td>Australian BioCommons (Not a Member)</td>
<td>Australian BioCommons</td>
</tr>
<tr>
<td>Threaten Species Initiative (Not a Member)</td>
<td>Threaten Species Initiative</td>
</tr>
<tr>
<td>University of Melbourne Centre for Cancer Research (Not a Member)</td>
<td>University of Melbourne Centre for Cancer Research</td>
</tr>
<tr>
<td>Zero Childhood Cancer (Not a Member)</td>
<td>Zero Childhood Cancer</td>
</tr>
</tbody>
</table>

The Australian BioCommons is supported by Bioplatforms Australia. Bioplatforms Australia is enabled by NCRIS.
“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

<table>
<thead>
<tr>
<th>Name</th>
<th>Client ID</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patto Test</td>
<td>ciologon/client_id/2e91851f6427452bea1eec8d0a16991c</td>
<td><img src="edit.png" alt="Edit" /> <img src="delete.png" alt="Delete" /></td>
</tr>
<tr>
<td>Test 01</td>
<td>ciologon/client_id/ebe66e1c90a0160e478aba98fa4f6f4</td>
<td><img src="edit.png" alt="Edit" /> <img src="delete.png" alt="Delete" /></td>
</tr>
<tr>
<td>UMCCR Data Commons (DEV)</td>
<td>ciologon/client_id/2d0a547d421d74a9cd87b0a21fca22ef</td>
<td><img src="edit.png" alt="Edit" /> <img src="delete.png" alt="Delete" /></td>
</tr>
</tbody>
</table>

The Australian BioCommons is supported by Bioplatforms Australia. Bioplatforms Australia is enabled by NCRIS.
First commit of CILogon authentication #896

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

skoranda commented on Apr 8 • edited by paulineribyre

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 (OIDD) 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 (OIDD) client registration is available to researchers and scholars at https://cilogon.org/oauth2/register
Global Authz Interoperability

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.”
Success!

- Show/Hide User Info

```javascript
{
  "sub": "http://cilogon.org/serverT/users/27326098",
  "idp_name": "University of Illinois at Urbana-Champaign",
  "epgn": "skoranda@illinois.edu",
  "cert subject dn": "/DC=org/DC=cilogon/C=US/O=University of Illinois at Urbana-Champaign/CN=Scott Koranda T27326098",
  "epnid": "urn:mace:incommon:uiuc.edu!https://cilogon.org/shibboleth!3fsruagzhH47ZBOQfjawaXGRnFV8",
  "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/demo8",
  "idp": "urn:mace:incommon:uiuc.edu",
  "token_id": "https://test.cilogon.org/oauth2/id token/7361b76e653124b750b98698b6b676fc41b/162704417974",
  "affiliation": "staff@illinois.edu; employee@illinois.edu; member@illinois.edu",
  "name": "Scott Koranda",
  "trustui": "65962BB827",
  "family_name": "Koranda",
  "gagslh_password_v1": [
    "eyJoeXAI01JKI1VnIiLICJa1mQ11t1YNDRCMM1rjZCMjMzR0ENzZM2kM0RSISlS5fSsYj1G1L1KMsU1In0.YeJ0zDI10j0dJH10w18vY21sb2vbi5vcnmcvc2Yd",
    "eyJoeXAI01JKI1VnIiLICJa1mQ11t1YNDRCMM1rjZCMjMzR0ENzZM2kM0RSISlS5fSsYj1G1L1KMsU1In0.YeJ0zDI10j0dJH10w18vY21sb2vbi5vcnmcvc2Yd",
    "eyJoeXAI01JKI1VnIiLICJa1mQ11t1YNDRCMM1rjZCMjMzR0ENzZM2kM0RSISlS5fSsYj1G1L1KMsU1In0.YeJ0zDI10j0dJH10w18vY21sb2vbi5vcnmcvc2Yd"
  ],
  "email": "skoranda@illinois.edu",
  "cid": "cilogon:test.cilogon.org/demo8"
}
```

- 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

* SciTokens support coming in 2020
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

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
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-SPproxies 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

<table>
<thead>
<tr>
<th>voPersonApplicationUID</th>
<th>voPersonExternalUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>voPersonAuthorName</td>
<td>voPersonID</td>
</tr>
<tr>
<td>voPersonCertificateDN</td>
<td>voPersonSoRlDN</td>
</tr>
<tr>
<td>voPersonCertificateIssuerDN</td>
<td>voPersonStatus</td>
</tr>
</tbody>
</table>
Zoom Survey!
Thank you.

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