CILogon
Enabling Federated Identity and Access Management for Scientific Collaborations

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

ClLogon (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.
Top 20 IdPs
(by # of unique active users in March 2022)

1315 Penn State
725 XSEDE
720 University of Illinois at Urbana-Champaign
665 Fermi National Accelerator Laboratory
619 National Institutes of Health
514 LIGO Scientific Collaboration
486 Northeastern University
483 University of Michigan
423 University of California-Los Angeles
420 Michigan State University
325 MIT
302 University of Chicago
297 Washington University in St. Louis
264 NCSA
255 Stanford University
251 Purdue University Main Campus
240 University of Wisconsin-Madison
216 Northwestern University
208 University of California-San Diego
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 restarted in 5 seconds now versus 15 minutes."
Federation support of research and scholarly communities

- Enable basic collaboration
- Support access to high value resources
- Protect collaboration resources

Reduce risk

Signal MFA
Signal identity assurance info

“Research & Scholarship” program
- Basic security
- Error handling
- Accurate & complete metadata for good user experience

Shared federation legal, policies and practices help collaborations manage risk

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

*slide courtesy Tom Barton*
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
examples of CILogon-enabled sites

“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/
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.

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.
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.

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

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 [link]</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 [link]</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.
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

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

https://github.com/jupyterhub/oauthenticator

CILogon
www.cilogon.org
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/
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

duPersonAffiliation: 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
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
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

<table>
<thead>
<tr>
<th>voPersonApplicationUID</th>
<th>voPersonExternalID</th>
</tr>
</thead>
<tbody>
<tr>
<td>voPersonAuthorName</td>
<td>voPersonID</td>
</tr>
<tr>
<td>voPersonCertificateDN</td>
<td>voPersonSoRID</td>
</tr>
<tr>
<td>voPersonCertificateIssuerDN</td>
<td>voPersonStatus</td>
</tr>
</tbody>
</table>

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 (UMCCCR)  
“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”

www.cilogon.org
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.”
Australian BioCommons

Home > University of Melbourne Centre for Cancer Research > OIDC Clients

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/2e91851f6427452bea1eec8d0a1699c</td>
<td>Edit, Delete</td>
</tr>
<tr>
<td>Test 01</td>
<td>ciologon/client_id/eba66e1c90a0160e478aba8fa4f6d4</td>
<td>Edit, Delete</td>
</tr>
<tr>
<td>UMCCCR Data Commons (DEV)</td>
<td>ciologon/client_id/2d9a547d421d74a9cd87b0a21fca226f</td>
<td>Edit, Delete</td>
</tr>
</tbody>
</table>

The Australian BioCommons is supported by Bioplatforms Australia. Bioplatforms Australia is enabled by NCRIS.
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
Global Authz Interoperability

Global Alliance
for Genomics & Health
Collaborate. Innovate. Accelerate.

GA4GH Passports
and the Authorization and Authentication Infrastructure
“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

```json
{
  "sub": "http://cilogon.org/serverT/users/27326998",
  "idp_name": "University of Illinois at Urbana-Champaign",
  "epnn": "skoranda@illinois.edu",
  "cert subject dn": "/DC=org/DC=cilogon/C=US/O=University of Illinois at Urbana-Champaign/CN=Scott Koranda T27326998",
  "eptid": "urn:mace:incommon:uiuc.eduhttps://cilogon.org/shibboleth!3fsruaqzH47Z80QfjwaXGKrnFVR8=",
  "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/idToken/7361b76653124b76098696b67676fc41bf/162704417947",
  "affiliation": "staff@illinois.edu;employee@illinois.edu;member@illinois.edu",
  "name": "Scott Koranda",
  "trustui": "698628827",
  "family_name": "Koranda",
  "gadgh_password v1": [
    "eyJ6eXAiOiJvIjoiLCJraWQiOiJyNDRCMjMlRjZCMjhfMzMzMDhEMTAXRUFDzNzN1MkM0RTSSImFsZyI6IjTMjU2In0.eyJzdWI1IjoidHRwOi8vY2lsb2dvbi5vcmcvd2VycyJ9",
    "eyJ6eXAiOiJvIjoiLCJraWQiOiJyNDRCMjMlRjZCMjhfMzMzMDhEMTAXRUFDzNzN1MkM0RTSSImFsZyI6IjTMjU2In0.eyJzdWI1IjoidHRwOi8vY2lsb2dvbi5vcmcvd2VycyJ9",
    "eyJ6eXAiOiJvIjoiLCJraWQiOiJyNDRCMjMlRjZCMjhfMzMzMDhEMTAXRUFDzNzN1MkM0RTSSImFsZyI6IjTMjU2In0.eyJzdWI1IjoidHRwOi8vY2lsb2dvbi5vcmcvd2VycyJ9"
  ],
  "email": "skoranda@illinois.edu",
  "cid": "cilogon:test.cilogon.org/demo8"
}
```

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