

# *CILogon*

**Identity and Access Management for Research Collaborations**

Scott Koranda  
skoranda@illinois.edu



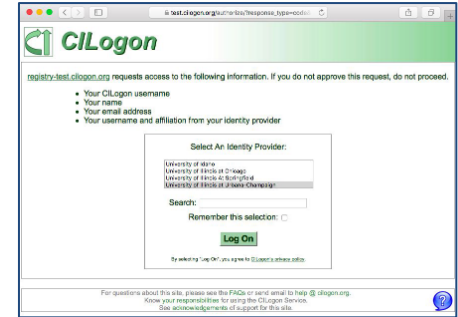
# IAM for Research Collaborations

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

Using federated identities so researchers log on with their existing credentials from their home organization

Supporting 164,000+ active users from 1170+ organizations around the world\*

\*At least one authentication flow during 2024



# In The Beginning...

Suppose researchers could exchange their campus credential for an X.509 (proxy?) certificate to use on the “grid”?

# The Sun Sets on X.509

JUNE 2023

The <https://cilogon.org/oauth2/getcert> endpoint is deprecated. No longer available to new CILogon OpenID Connect (OAuth) clients

JANUARY 2024

The <https://cilogon.org/oauth2/getcert> endpoint is disabled

MAY 2025

The "Create Password-Protected Certificate" option at <https://cilogon.org/> will be disabled

AFTER MAY 2025

CILogon X.509 CAs will be retired and withdrawn from the IGTF distribution

# OIDC and OAuth2

CILogon provides a standards-compliant OpenID Connect (OAuth 2.0) interface to federated authentication for cyberinfrastructure

CILogon proxy translates SAML assertions (campuses) and OIDC claims (Google, GitHub, ORCID, Microsoft) to OIDC identity tokens and OAuth2 tokens

# Basic Authentication Tier

No charge for academic research projects

OpenID Connect Provider (with manual registration of clients at <https://cilogon.org/oauth2/register>)

Shibboleth SAML Service Provider (federated via InCommon)

Provided with best effort support (via [help@cilogon.org](mailto:help@cilogon.org))

~2000 OIDC clients

# Last 10\* Basic Authentication Clients

NRP User Dev Environment (Jupyter)

Future Water Login

UNR CSE

Cal State Fullerton (Jupyter)

Yeti (Woods Hole Oceanographic)

UAT Testing (U Alberta)

Data.Ai (UKY)

IceCube Indico

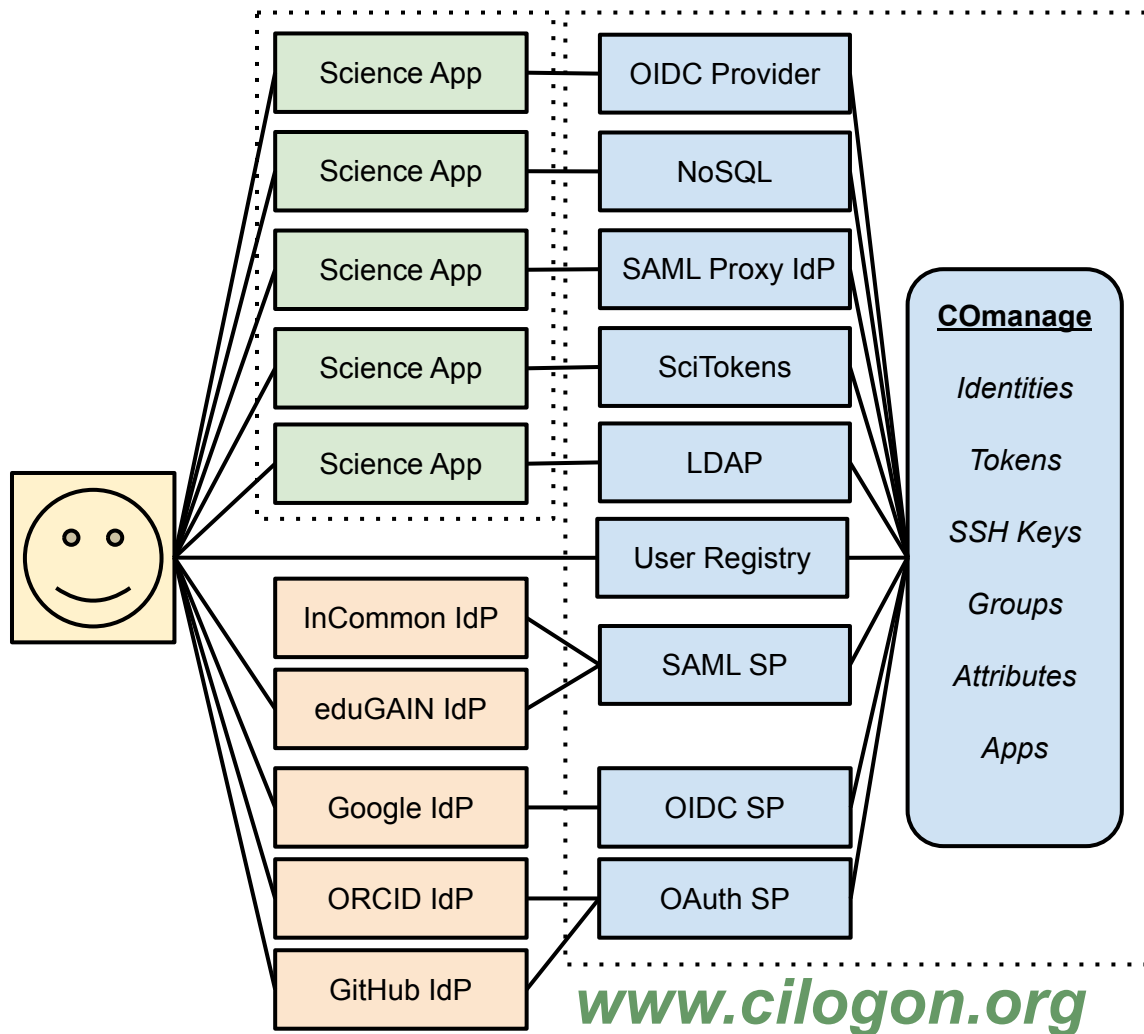
CAT-Talk (UKY)

HackInSDN - UFBA

\*Since 11/18/24

# Identity Management for Research and Scholarship as a Hosted Service

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





# Essential Service Tier

\$15,759 per year

OpenID Connect Provider (with client management via CManage and OAuth API)

Shibboleth SAML Service Provider (federated via InCommon, with support for custom configurations)

CManage Registry (multi-tenant instance for up to 5 COs with CO Admin access at <https://registry.cilogon.org/>)

OpenLDAP Directory

SATOSA SAML Proxy

pyFF MDQ Server

Customized CILogon.org Login page

Federated access to AWS, Azure, Google Cloud, and IBM Cloud

Provided under a detailed service level agreement

# Full Service Tier

\$36,771 per year

OpenID Connect Provider (with client management via CManage and OAuth API)  
Shibboleth SAML Service Provider (federated via InCommon, with support for custom configurations)  
X.509 Certification Authority services (scheduled for retirement)  
CManage Registry (dedicated with custom DNS name, unlimited COs, support for custom plug-ins, and CO Admin access)  
OpenLDAP Directory  
SATOSA SAML Proxy and pyFF MDQ Server  
Customized CILogon.org Login page  
Federated access to AWS, Azure, Google Cloud, and IBM Cloud  
JWT Issuer supporting SciTokens, WLCG Tokens, RFC 9068, and GA4GH Passports with custom configurations

Additional support channels: Zoom calls, dedicated Slack channels

Provided under a detailed service level agreement

# Subscribers

ACCESS

LSST

NCSA Business IT, Magnus, HAL, vForge

Illinois Computes

LIGO/Virgo/KAGRA/IGWN

RENCI@UNC (FABRIC, ImPACT)

BNL (DCDE/SDCC)

Morgridge (OSG)

Fermilab

UCSD (CloudBank)

Flywheel

AU Biocommons

AU CADRE

AU LDaCA

JLab

U of Colorado - Boulder (RMACC)

2I2C

U of Washington (NACC)

University of Missouri

Digital Research Alliance of Canada

LBNL (SAFER)

Syracuse (Cosmic Explorer)

Positron Networks

# Amazon Web Services

Relational Database Service

Elastic File System

Elastic Kubernetes System (ec2)

Certificate Service

IAM

DynamoDB

# Amazon Web Services

us-east-2 (Ohio)

ap-southeast-2 (Sydney)

ca-central-1 (Canada central) soon?

\$3122 November 2024

# CILogon Team

Jim Basney

Robin Blair

Terry Fleury

Jeff Gaynor

Scott Koranda

Yan Zhan

~ 3.5 FTE

# Tokens for Science

## OpenID Connect (OIDC) ID Tokens

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)



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

# Token Standards

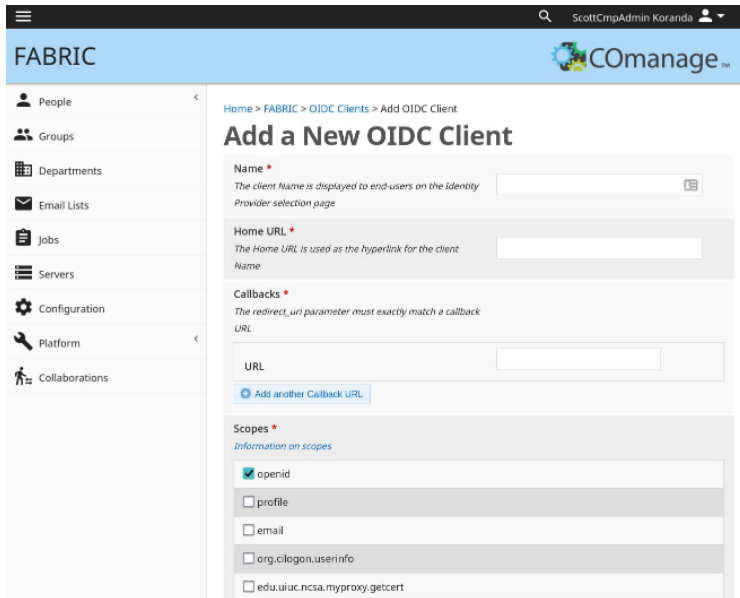
- RFC 6749: OAuth 2.0 Authorization Framework
  - token request, consent, refresh
- RFC 7519: JSON Web Token (JWT)
  - self-describing tokens, distributed validation
- RFC 8414: OAuth 2.0 Authorization Server Metadata
  - token signing keys, policies, endpoint URLs
- RFC 8693: OAuth 2.0 Token Exchange
  - 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>



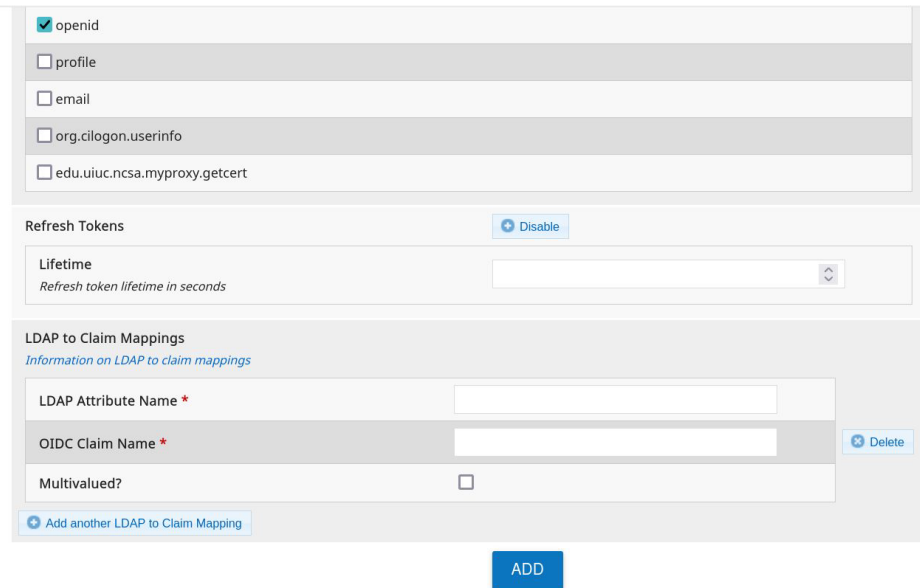
# Managing OIDC & OAuth2 Apps

## Subscribers manage apps using CManage



The screenshot shows the 'Add a New OIDC Client' form in the CManage interface. The breadcrumb trail is 'Home > FABRIC > OIDC Clients > Add OIDC Client'. The form includes the following sections:

- Name \***: A text input field with a note: 'The client Name is displayed to end-users on the identity Provider selection page'.
- Home URL \***: A text input field with a note: 'The Home URL is used as the hyperlink for the client Name'.
- Callbacks \***: A section with a note: 'The redirect\_uri parameter must exactly match a callback URL'. It contains a 'URL' input field and a '+ Add another Callback URL' button.
- Scopes \***: A section with a note: 'Information on scopes'. It contains a list of checkboxes: 'openid' (checked), 'profile', 'email', 'org.cilogon.userinfo', and 'edu.uiuc.ncsa.myproxy.getcert'.



The screenshot shows the 'Refresh Tokens' and 'LDAP to Claim Mappings' sections of the CManage interface.

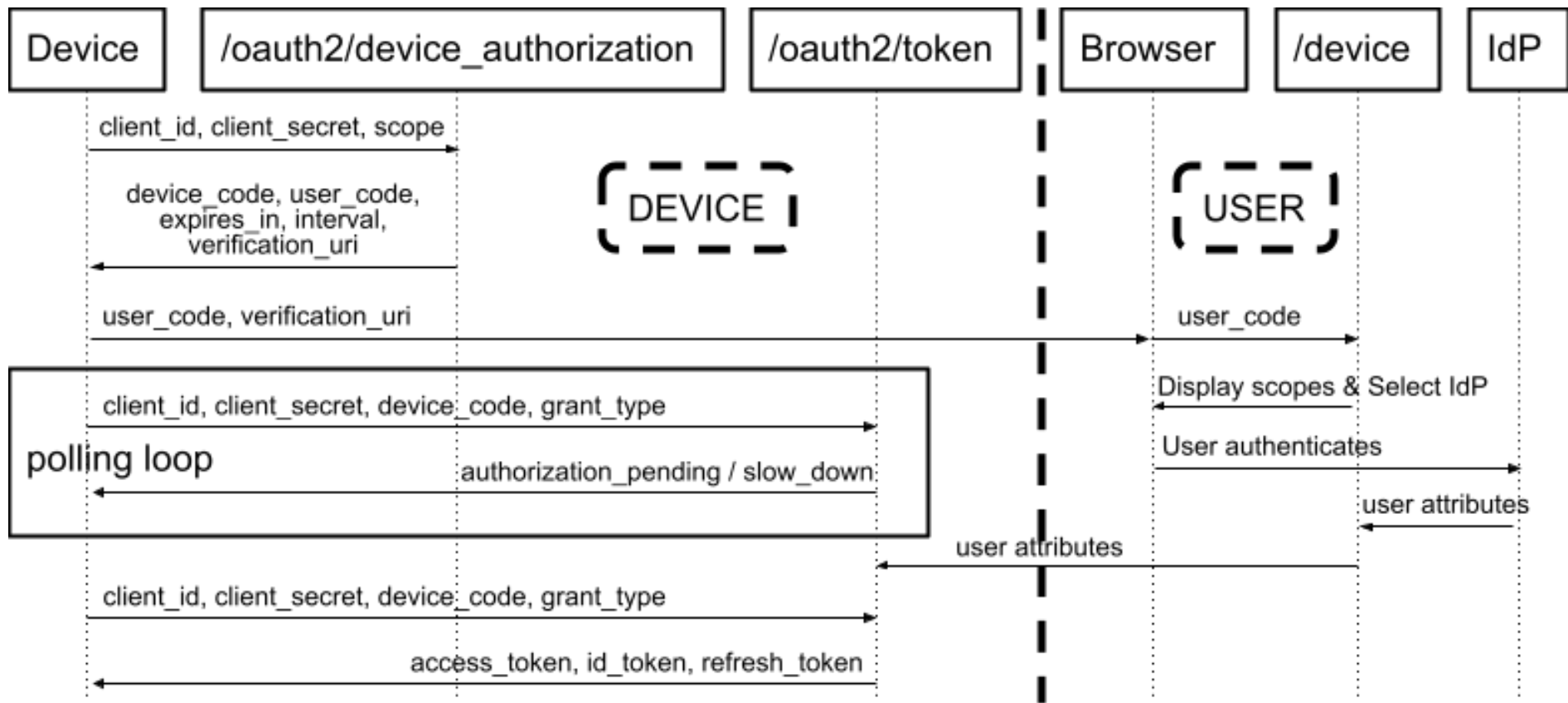
- Refresh Tokens**: A section with a '+ Disable' button. It contains a 'Lifetime' dropdown menu with a note: 'Refresh token lifetime in seconds'.
- LDAP to Claim Mappings**: A section with a note: 'Information on LDAP to claim mappings'. It contains a table with two rows: 'LDAP Attribute Name \*' and 'OIDC Claim Name \*', each with an input field. A 'Delete' button is next to the second row. There is also a 'Multivalued?' checkbox and a '+ Add another LDAP to Claim Mapping' button.

An 'ADD' button is located at the bottom right of the form.

# 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



# Challenges

# Attribute Release

CILogon

## Attribute Release Error



There was a problem logging on. Your identity provider has not provided CILogon with required information.

|                       |         |
|-----------------------|---------|
| <b>subject-id:</b>    | MISSING |
| <b>ePPN:</b>          | MISSING |
| <b>First Name:</b>    | MISSING |
| <b>Last Name:</b>     | MISSING |
| <b>Display Name:</b>  | MISSING |
| <b>Email Address:</b> | MISSING |

Contact your identity provider to let them know you are having having a problem logging on to CILogon.

- Support Contact: UC Davis IT Express [ithelp@ucdavis.edu](mailto:ithelp@ucdavis.edu)

Alternatively, you can contact us at the email address at the bottom of the page.

Proceed

# Attribute Release

Hello, I am having trouble logging on to <https://cilogon.org/> using the Northeastern University Identity Provider (IdP) with Globus due to the following missing attributes:

subject-id -OR-  
eduPersonPrincipalName  
givenName (first name)  
sn (last name)  
displayName  
mail (email address)

Please see <https://www.cilogon.org/service/addidp> for more details. Thank you for any help you can provide.

# IdP EntityID Changes

EntityID and combination of persistent identifiers maps uniquely to a user

Right now when EntityID changes (without warning) RPs see a “new” user

We will be dropping entityID and using `<shibmd:Scope>` instead.

# SAML subject-id Attribute

1171 IdPs used since Jan 01, 2024 to date

Of those IdPs 52 asserted SAML subject-id

~4.4%



# Questions?