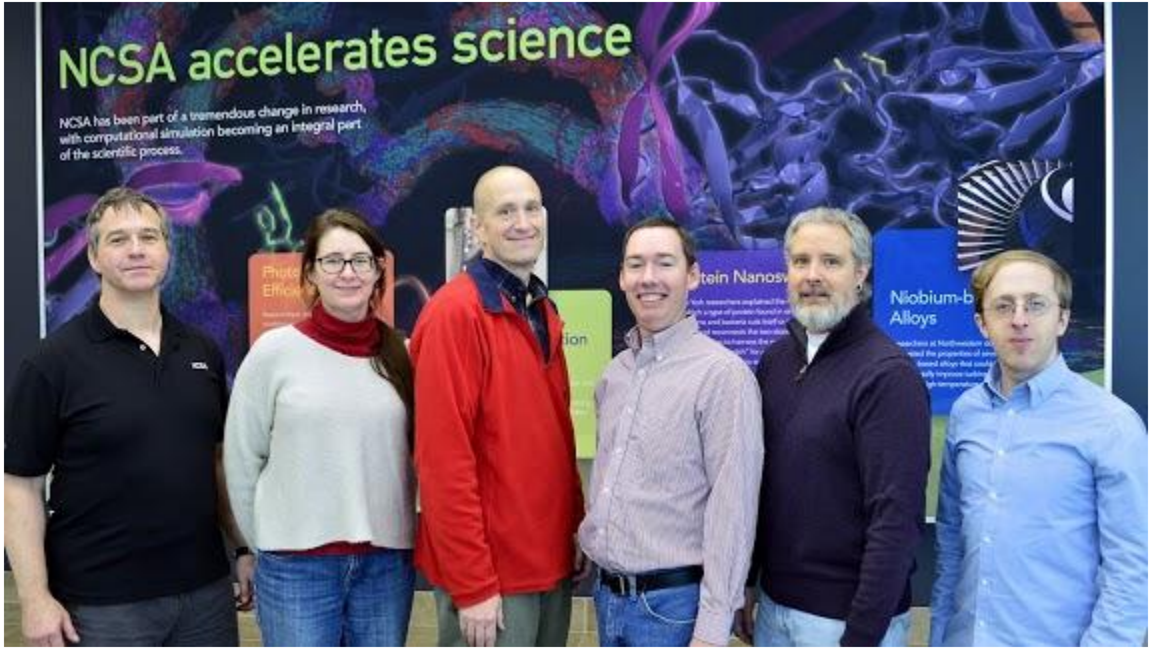
CILogon

Enabling Federated Identity and Access Management for Scientific Collaborations

Jim Basney
jbasney@ncsa.illinois.edu

April 2019

who we are


NCSA accelerates science
NCSA has been part of a tremendous change in research, with computational simulation becoming an integral part of the scientific process.
Niobium-b
Alloys

ncsa.illinois.edu sphericalcowgroup.com

our vision

enable logon to scientific cyberinfrastructure (CI)

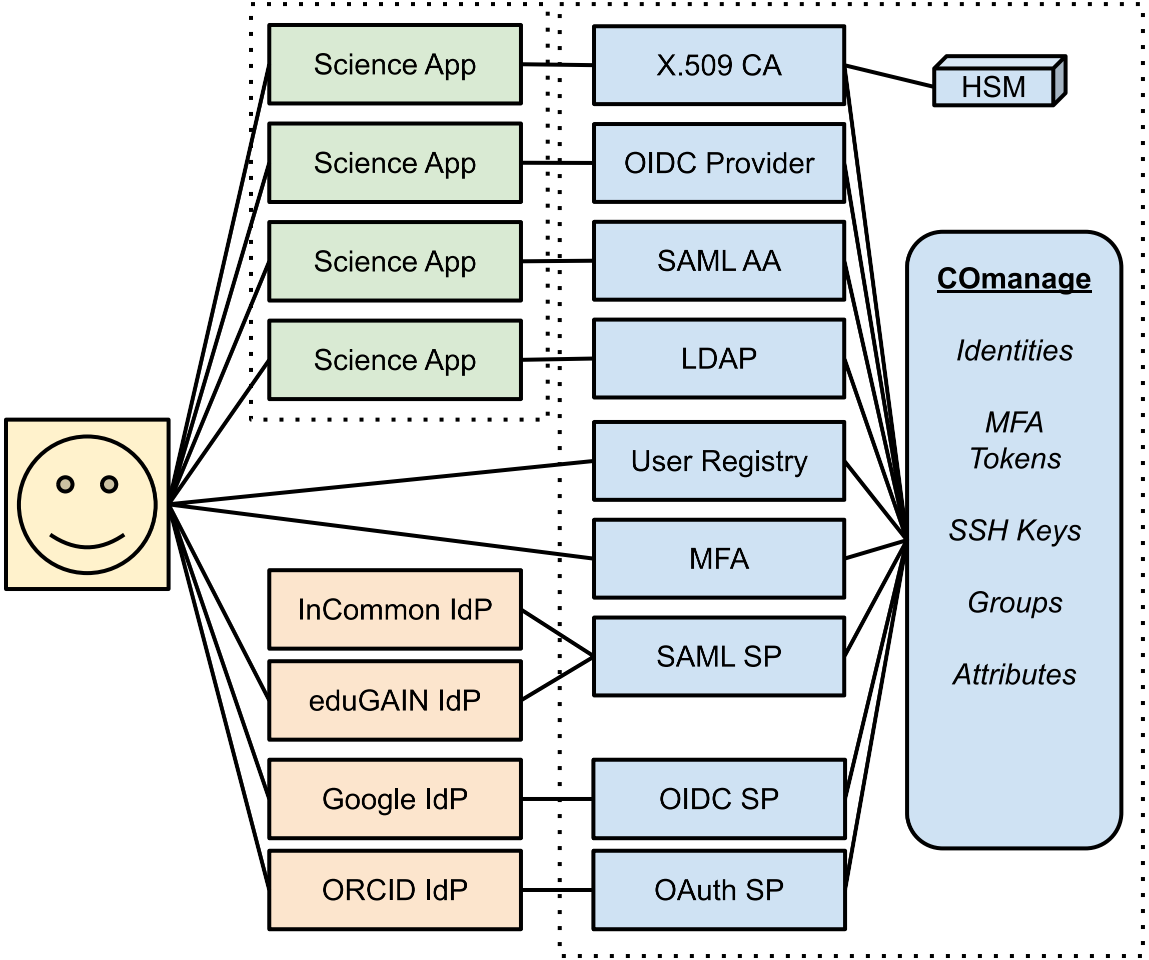
seamless IAM for academic research collaborations

use your campus identity (eduGAIN/Shibboleth)

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

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

federated identity management and collaborative organization management



realizing our vision

- align with Internet2 TIER (https://www.internet2.edu/tier)
  - 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
- TIER (https://www.internet2.edu/tier)
    - Shibboleth, COmanage, Grouper
- IdentityPython (https://idpy.org/)
    - pyFF, SATOSA
- OpenLDAP

enabling global interfederation

Research & Scholarship

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

Security Incident Response Trust Framework for Federated Identity

https://refeds.org/sirtfi

REFEDS

our baseline: REFEDS R&S

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

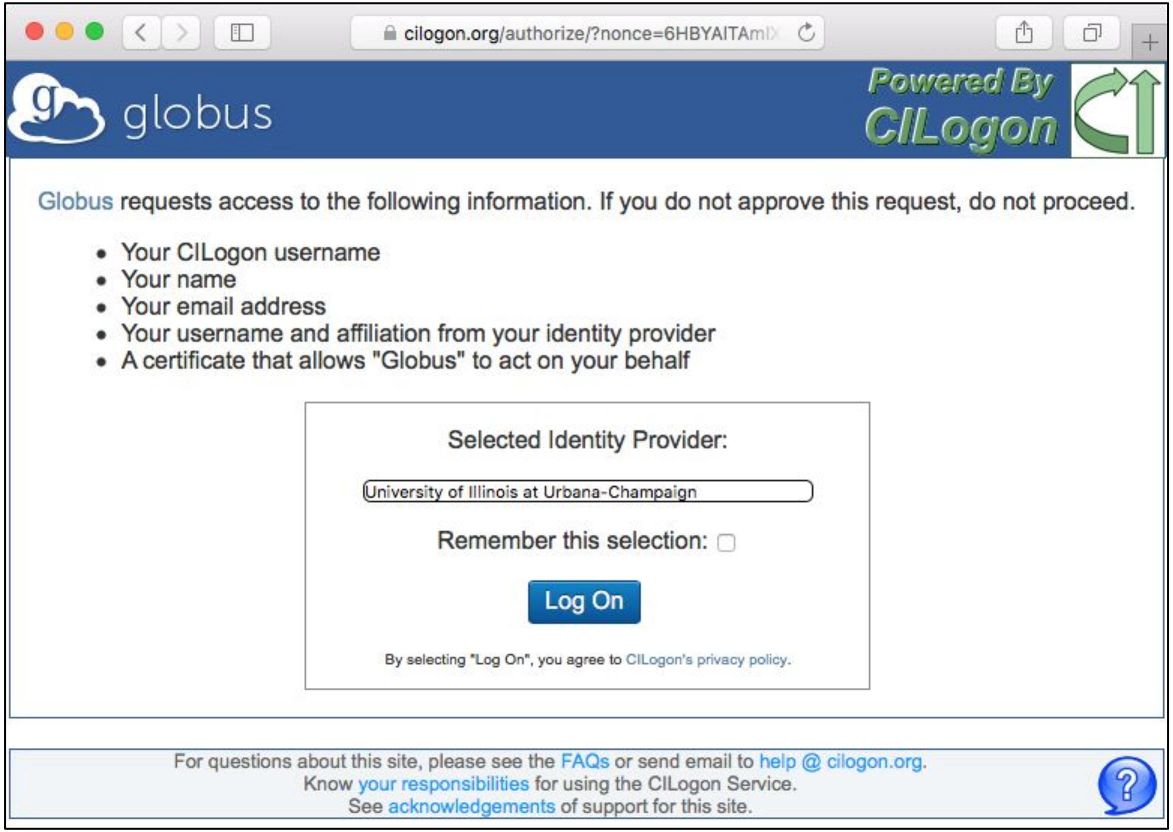
We operate under the REFEDS R&S policy.

Does your campus support REFEDS R&S?

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

https://test.cilogon.org/testidp/

informed consent



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

- 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

Selected Identity Provider:

University of Illinois at Urbana-Champaign

Remember this selection: □

Log On

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

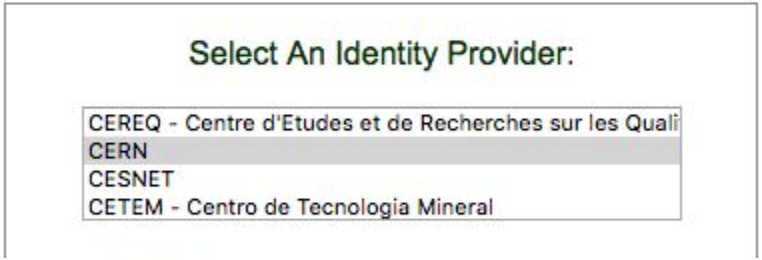
For questions about this site, please see the FAQs or send email to help @ cilogon.org.
Know your responsibilities for using the CILogon Service.
See acknowledgements of support for this site.

supporting global access

Thanks to eduGAIN!

CILogon policy update approved in 2016 by Interoperable Global Trust Federation

Requiring R&S + Sirtfi



Select An Identity Provider:

CEREQ - Centre d'Etudes et de Recherches sur les Quali
CERN
CESNET
CETEM - Centro de Tecnologia Mineral

IGTF
AP | EU | TAG

managing project groups/roles

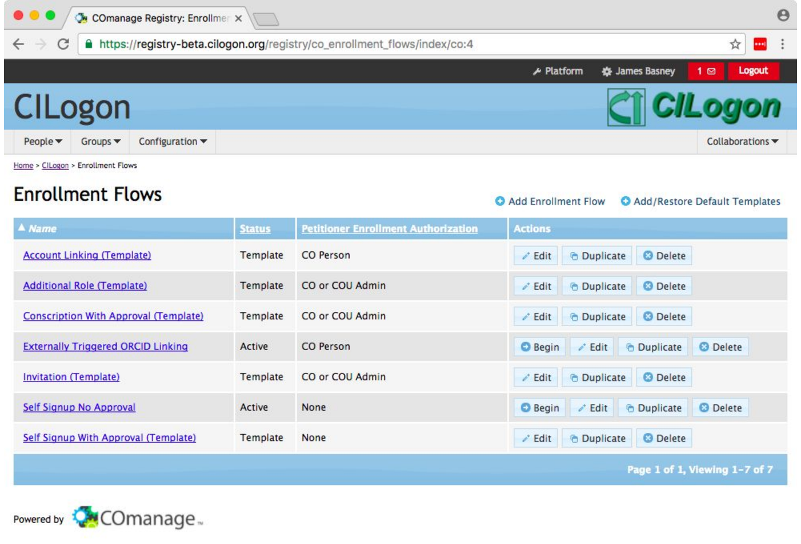
COmanage provides:

enrollment flows

expiration policies

self service permissions

pipelines



COmanage Registry: Enrollme
https://registry-beta.cilogon.org/registry/co_enrollment_flows/index/co:4
Platform
James Basney
1
Logout
CILogon
CILogon
People
Groups
Configuration
Collaborations

Home > CILogon > Enrollment Flows

Enrollment Flows

Add Enrollment Flow   Add/Restore Default Templates

▲ 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

COmanage™

collaboration management platform
built for federated identity

Open Source

Internet2/InCommon

PHP

Version 3.2.1

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

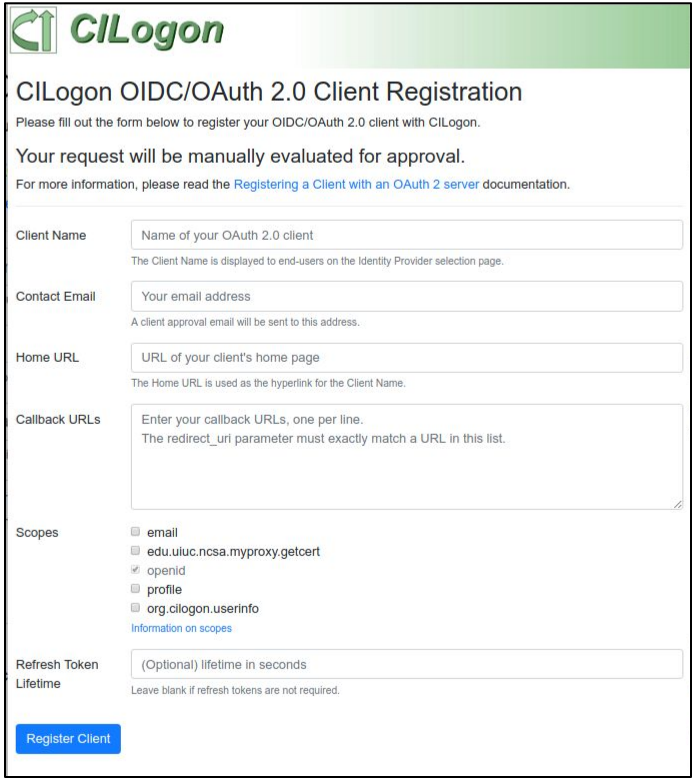
registering your OIDC app

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

including app details

save client_id
and client_secret

wait for notification
by help@cilogon.org



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:
- ☐ email
- ☐ edu.uiuc.ncsa.myproxy.getcert
- ☑ openid
- ☐ profile
- ☐ org.cilogon.userinfo

Information on scopes

Refresh Token Lifetime: (Optional) lifetime in seconds
Leave blank if refresh tokens are not required.

configuring your OIDC app

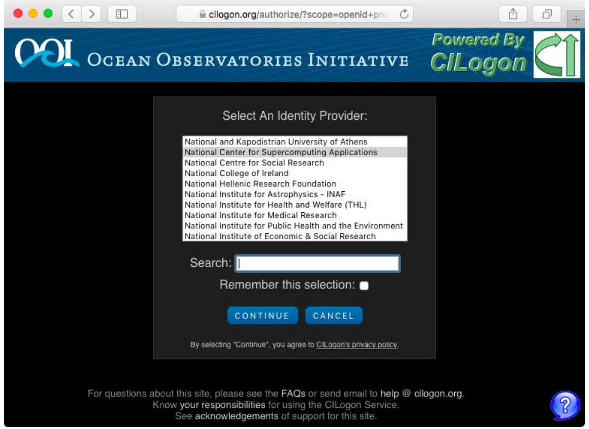
OIDC Discovery URL provides metadata

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

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

docs / examples:

http://www.cilogon.org/oidc



cilogon.org/authorize/?scope=openid+pro

OCEAN OBSERVATORIES INITIATIVE

Powered By CILogon

Select An Identity Provider:

National and Kapodistrian University of Athens
National Center for Supercomputing Applications
National Centre for Social Research
National College of Ireland
National Hellenic Research Foundation
National Institute for Astrophysics - INAF
National Institute for Health and Welfare (THL)
National Institute for Medical Research
National Institute for Public Health and the Environment
National Institute of Economic & Social Research

Search:

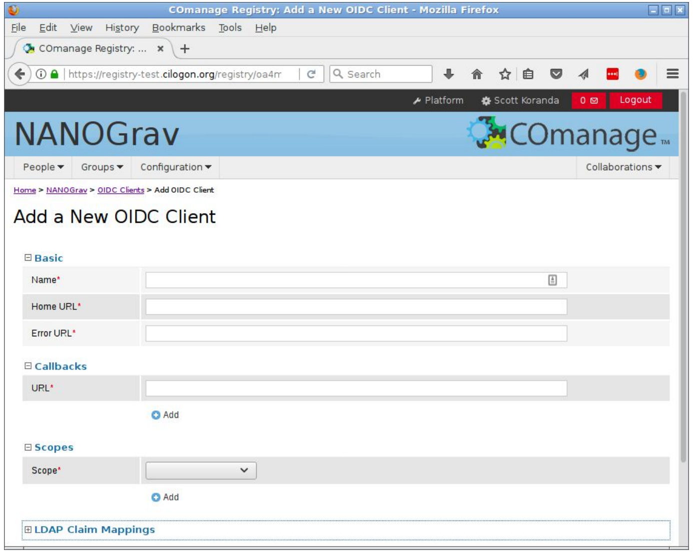
Remember this selection: □

By selecting "Continue", 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.

managing VO apps

enable VOs to register/manage their apps


COmanage Registry: Add a New OIDC Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://registry-test.cilogon.org/registry/oa4m
Search
Platform
Scott Koranda
0
Logout
NANOGrav
COmanage
People
Groups
Configuration
Collaborations

Home > NANOGrav > OIDC Clients > Add OIDC Client

Add a New OIDC Client

⊟ Basic

Name*	
Home URL*	
Error URL*	

⊟ Callbacks

URL*	

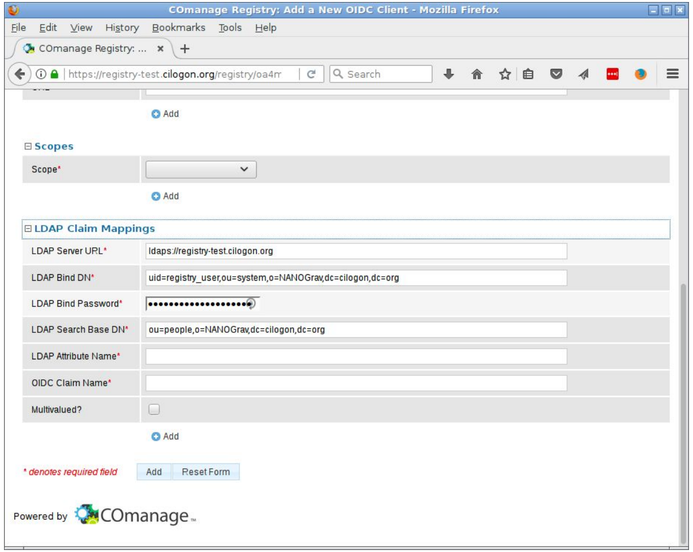
Add

⊟ Scopes

Scope*	

Add

⊞ LDAP Claim Mappings


COmanage Registry: Add a New OIDC Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://registry-test.cilogon.org/registry/oa4m
Search

Add

⊟ Scopes

Scope*	

Add

⊟ LDAP Claim Mappings

LDAP Server URL*	ldaps://registry-test.cilogon.org
LDAP Bind DN*	uid=registry_user,ou=system,o=NANOGrav,dc=cilogon,dc=org
LDAP Bind Password*	••••••••••••••••••••
LDAP Search Base DN*	ou=people,o=NANOGrav,dc=cilogon,dc=org
LDAP Attribute Name*	
OIDC Claim Name*	
Multivalued?	□

Add

** denotes required field*

Add | Reset Form

Powered by COmanage

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

campus & researcher IDs

2500+ 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

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

science gateways

enable web-based computational experiments and data management

CILogon-enabled hosted gateways:

Science Gateway Platform as a Service

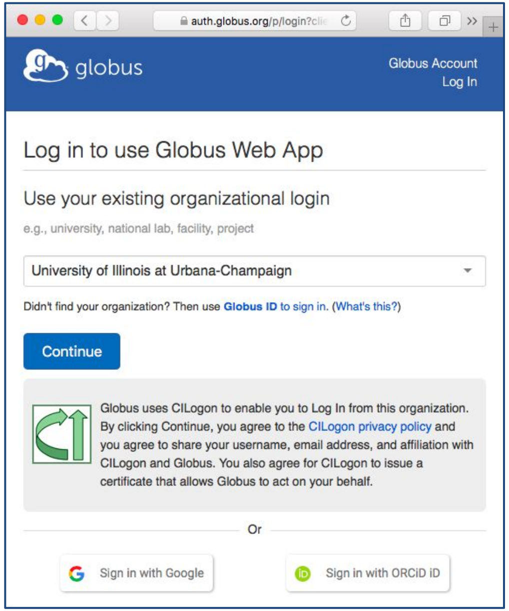
SciGaP

Globus

campus authentication to your Globus Data Transfer Node

- CILogonIdentityProvider option during Globus Connect Server install

campus identities for Globus Auth



auth.globus.org/p/login?clie

globus

Globus Account Log In

Log in to use Globus Web App

Use your existing organizational login

e.g., university, national lab, facility, project

University of Illinois at Urbana-Champaign

Didn't find your organization? Then use Globus ID to sign in. (What's this?)

Continue

Globus uses CILogon to enable you to Log In from this organization. By clicking Continue, you agree to the CILogon privacy policy and you agree to share your username, email address, and affiliation with CILogon and Globus. You also agree for CILogon to issue a certificate that allows Globus to act on your behalf.

Or

Sign in with Google

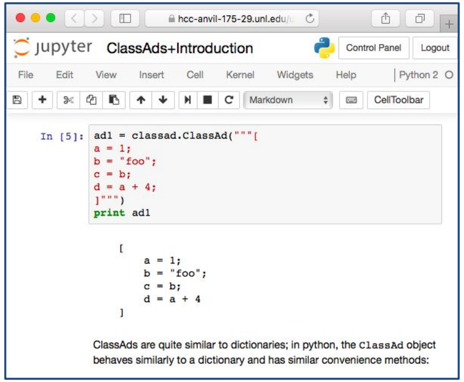
Sign in with ORCiD iD

JupyterHub

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

federated authentication using CILogon

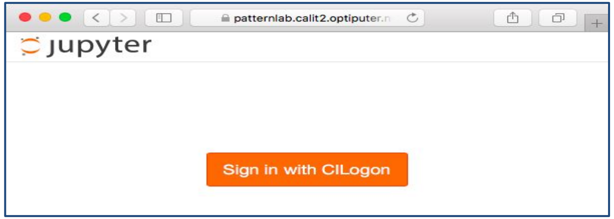
one IdP or many



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

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

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

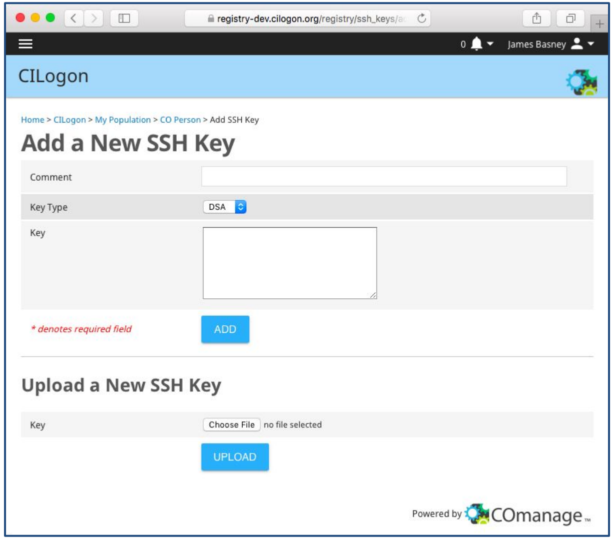
federated SSH keys

users register SSH public key during enrollment

associated with their federated identity

provisioned to LDAP

used by SSH server for authorization


registry-dev.cilogon.org/registry/ssh_keys/a
0
James Basney
CILogon
Home > CILogon > My Population > CO Person > Add SSH Key

Add a New SSH Key

Comment	
Key Type	DSA
Key	

* denotes required field

Upload a New SSH Key

Key	Choose File no file selected

UPLOAD
Powered by COmanage™

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

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.uits.iu.edu/

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.

sustainability

development supported by NSF/DOE

operational support from XSEDE

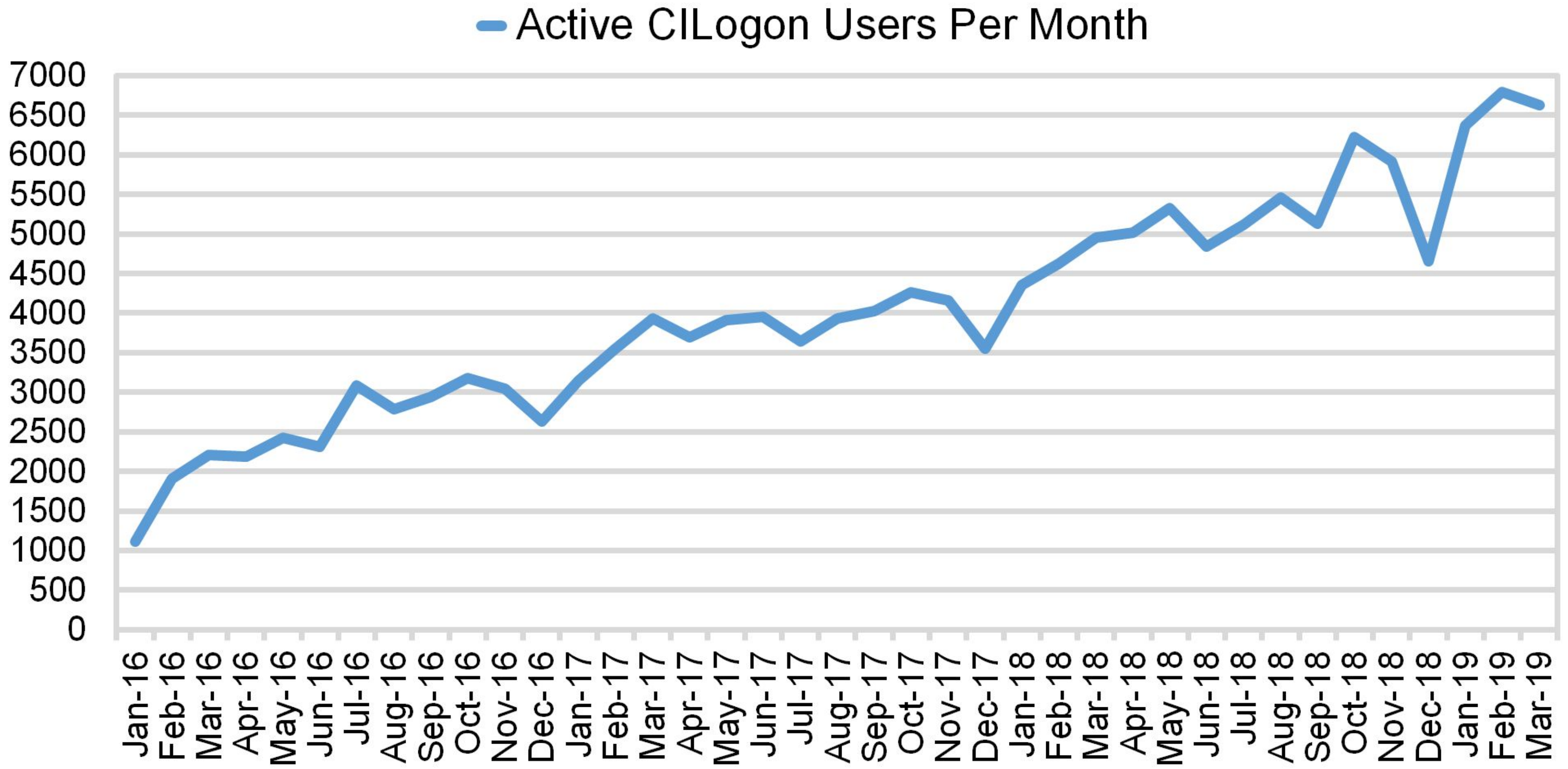
XSEDE
Extreme Science and Engineering
Discovery Environment

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



CILogon www.cilogon.org

Thanks!

contact:

help@cilogon.org

jbasney@ncsa.illinois.edu