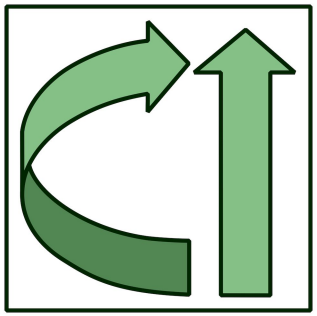
CILogon 2.0



Jim Basney
Scott Koranda

This material is based upon work supported by the National Science Foundation under grant numbers 0850557, 0943633, 1053575, 1440609, and 1547268 and by the Department of Energy under award number DE-SC0008597. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government or any agency thereof.

CILogon 2.0 Project

- 3 year NSF CICI award
  - January 2016 - December 2018
- Provide an integrated open source Identity and Access Management (IdAM) platform for cyberinfrastructure
  - CILogon: federated identity management
  - COmanage: collaborative organization management
- Support *international* collaborations

NSF CICI Program

- Cybersecurity Innovation for Cyberinfrastructure (CICI)
- Funds projects in the areas of
  - Cybersecurity Center of Excellence
  - Regional Cybersecurity Collaboration
  - Secure and Resilient Architecture
  - Secure Architecture Design
  - Data Provenance for Cybersecurity

https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=505159

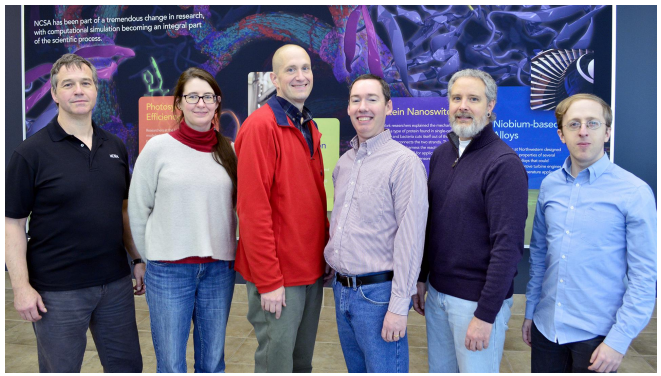
CILogon 2.0 Team Members

NCSA

MOO

spherical cow group

- Jim Basney
- Terry Fleury
- Jeff Gaynor
- Venkat Yekkirala
- Heather Flanagan
- Scott Koranda
- Benn Oshrin
- Arlen Johnson



Science Partners

- NANOGrav Physics Frontiers Center
- Laser Interferometer Gravitational-Wave Observatory (LIGO)
- Data Observation Network for Earth (DataONE)

Cyberinfrastructure Partners

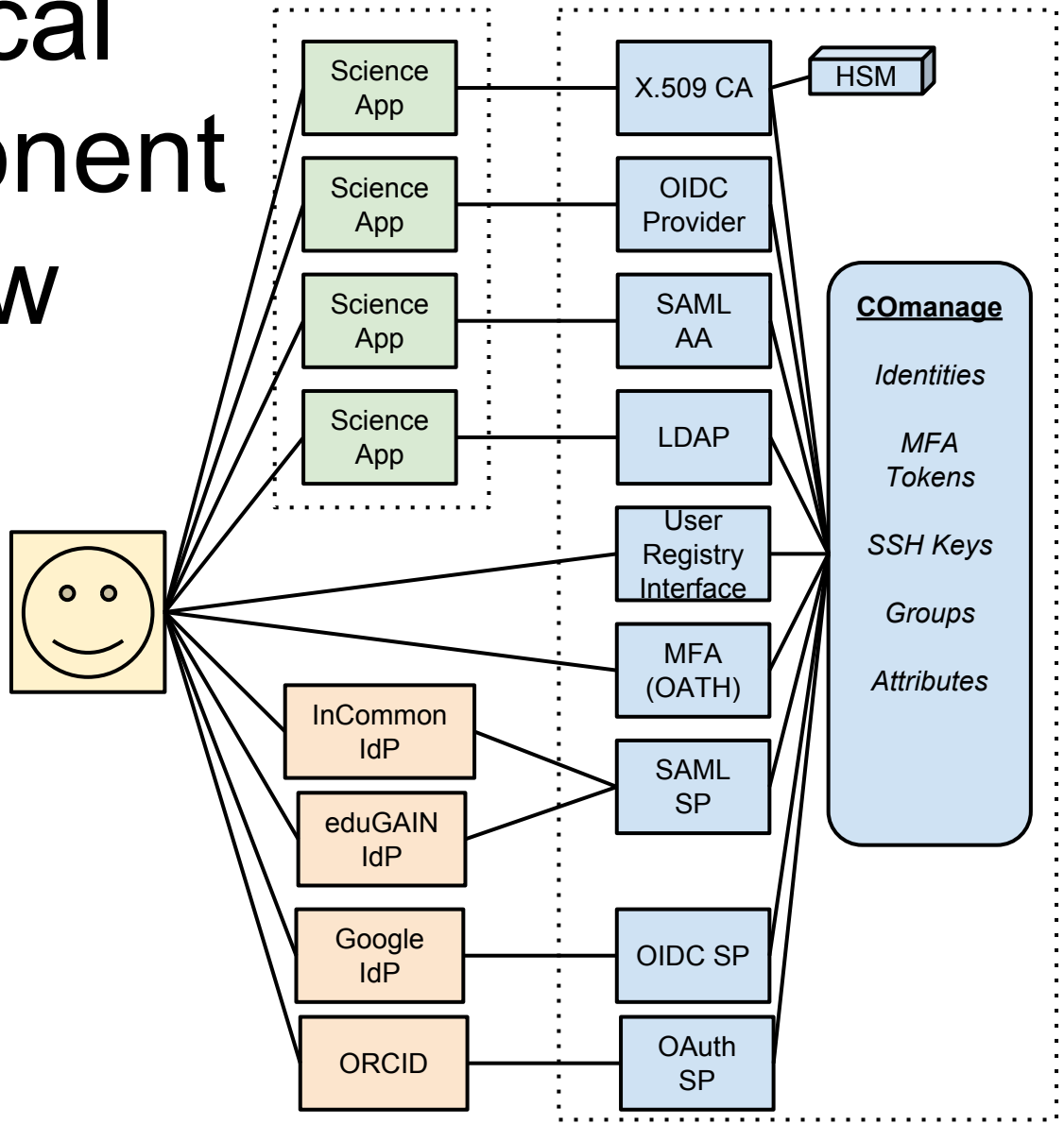
- Operational support
- Integration platform
- International use cases

- Support for European identities
- Using eduGAIN

CILogon in Europe

- Supporting international research collaborations
- Int'l IdP support at cilogon.org soon via InCommon's eduGAIN membership
  - Depends on int'l R&S adoption
- European CILogon instance
  - Addresses EU attribute release policies
  - IGTF accredited CA: https://rcauth.eu/

Logical Component View

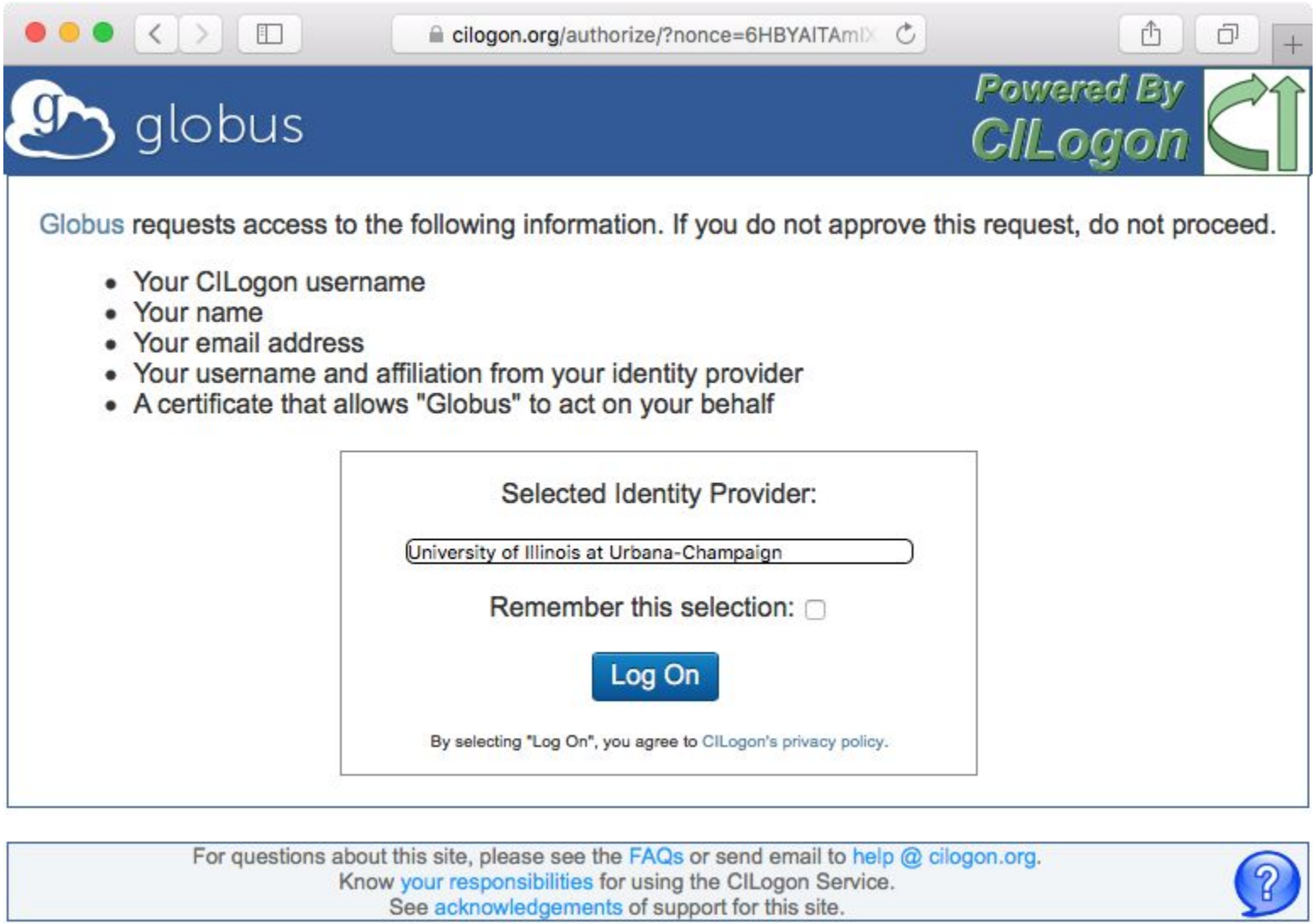


SAML to OpenID Connect (OIDC) Gateway

- Supporting e-Science clients
  - Review & approval by CILogon staff
- User consent based on requested scopes
  - openid, profile, email
  - org.cilogon.userinfo (eppn, affiliation)
  - edu.uiuc.ncsa.myproxy.getcert
    (to allow X.509 certificate issuance)
  - VO attributes

www.cilogon.org/oidc

CILogon User Consent



A Transparent Gateway

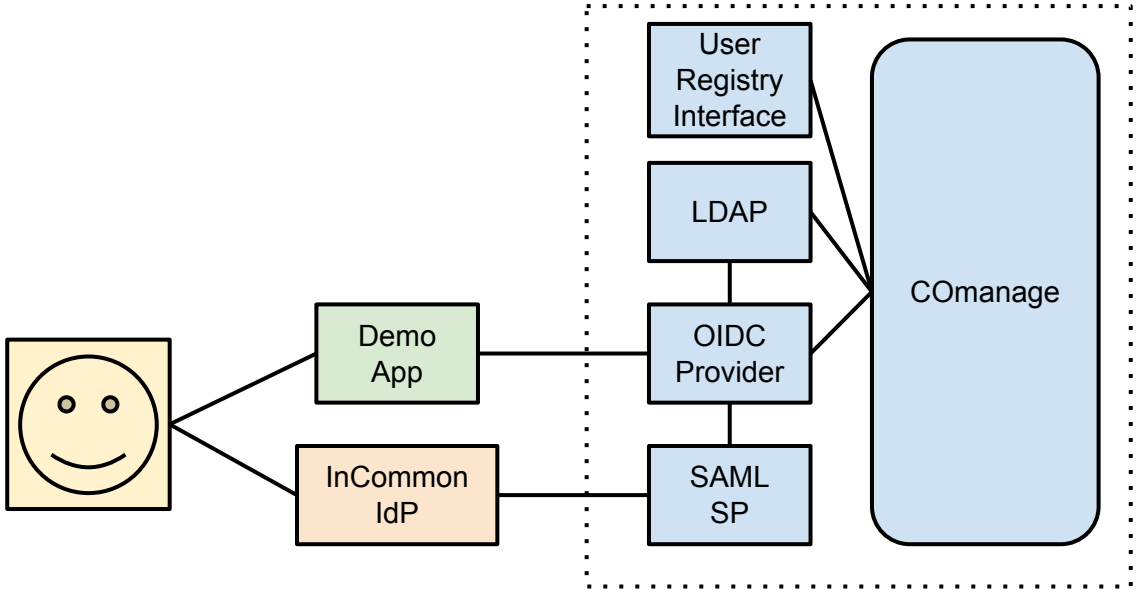
- CILogon passes campus/VO attributes to the e-Science SP
  - Always requiring user consent
  - Attribute scopes approved per-client
- COmanage displays terms and conditions during VO enrollment
  - VO attribute release policy applied per client

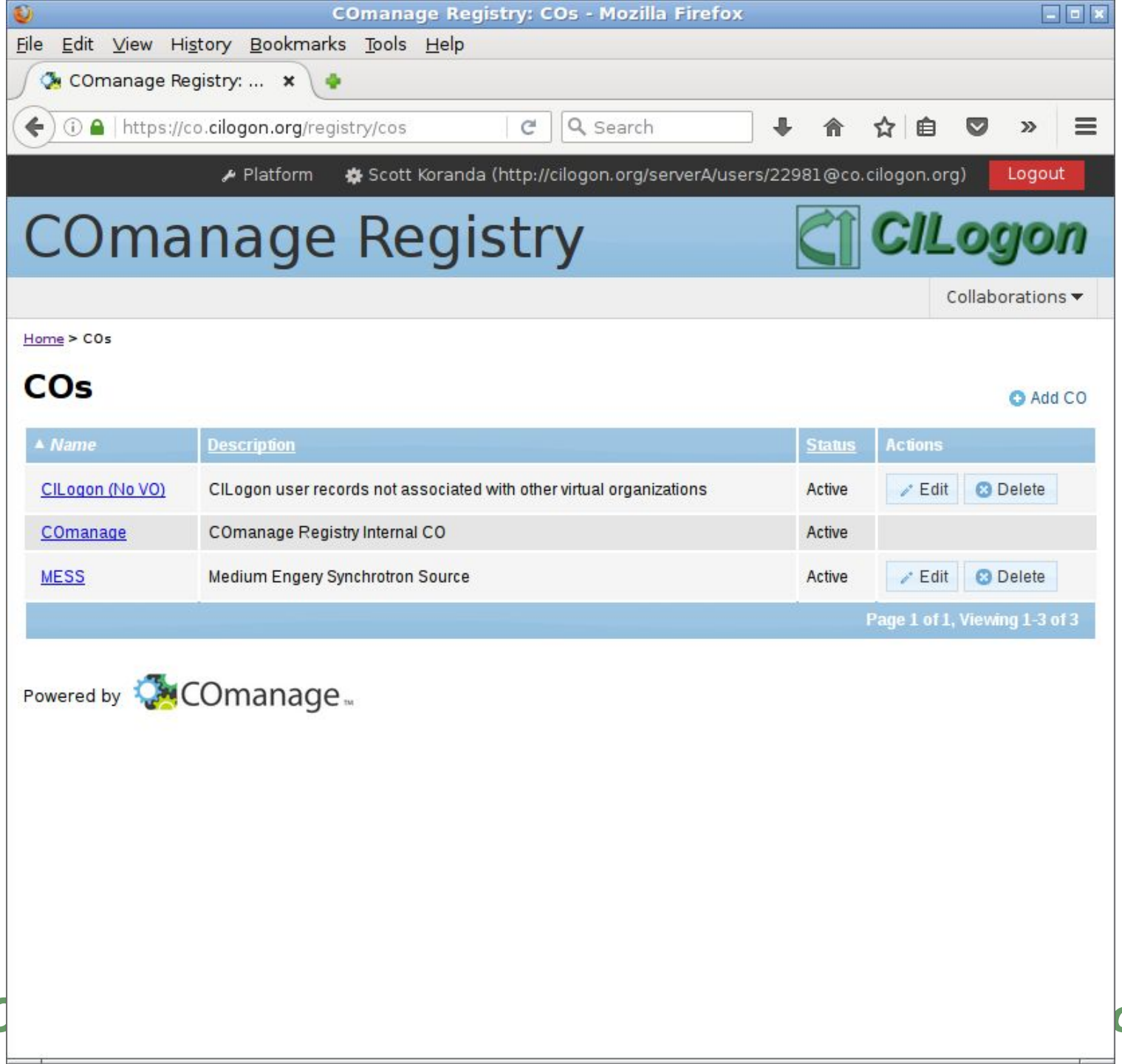
Open Researcher and Contributor ID (ORCID)

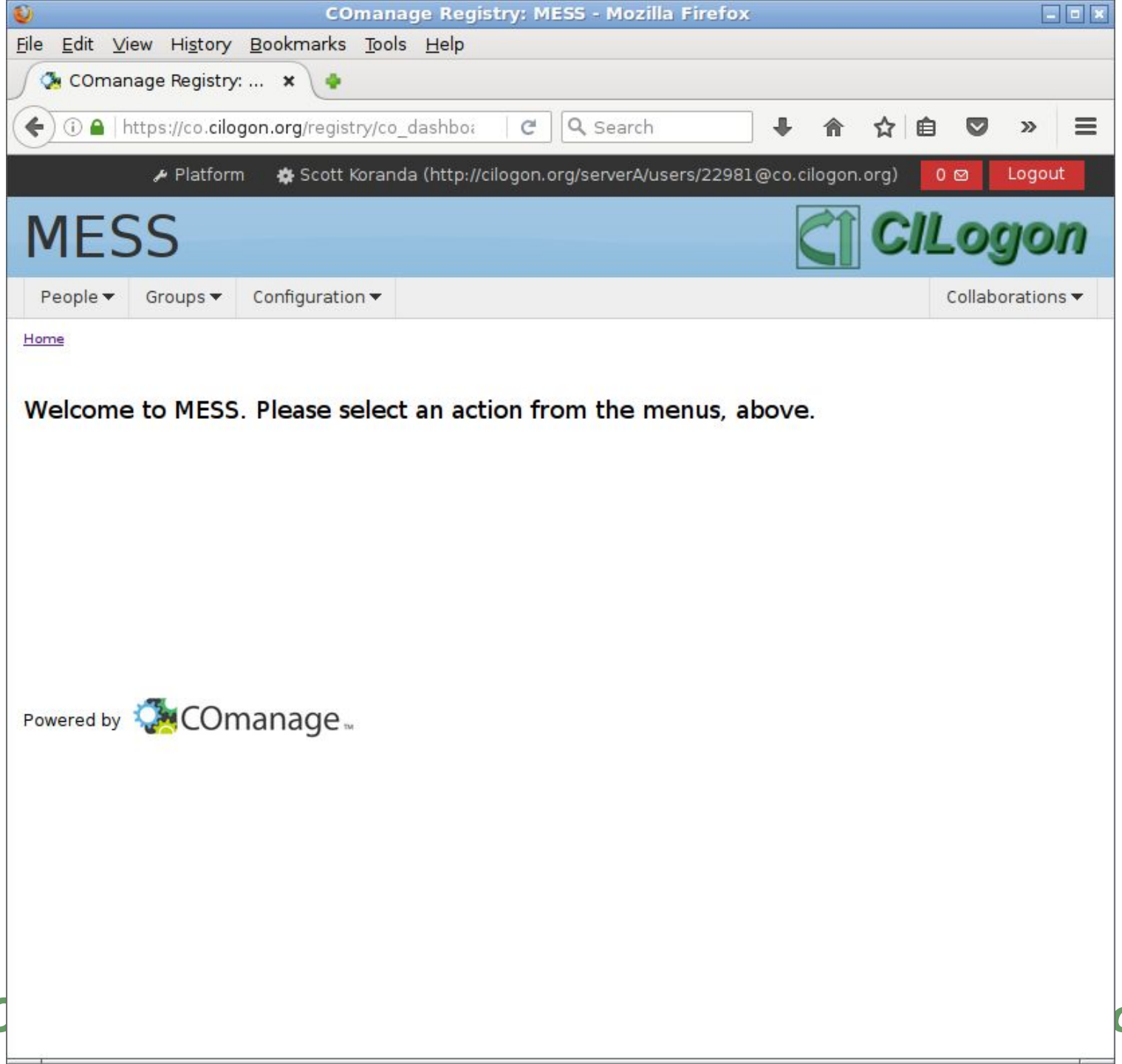
- Linking ORCID iDs to federated IDs
  - orcid.org
  - on campus
  - search.dataone.org
  - cilogon.org
- eduPersonOrcid
- REFEDS ORCID working group

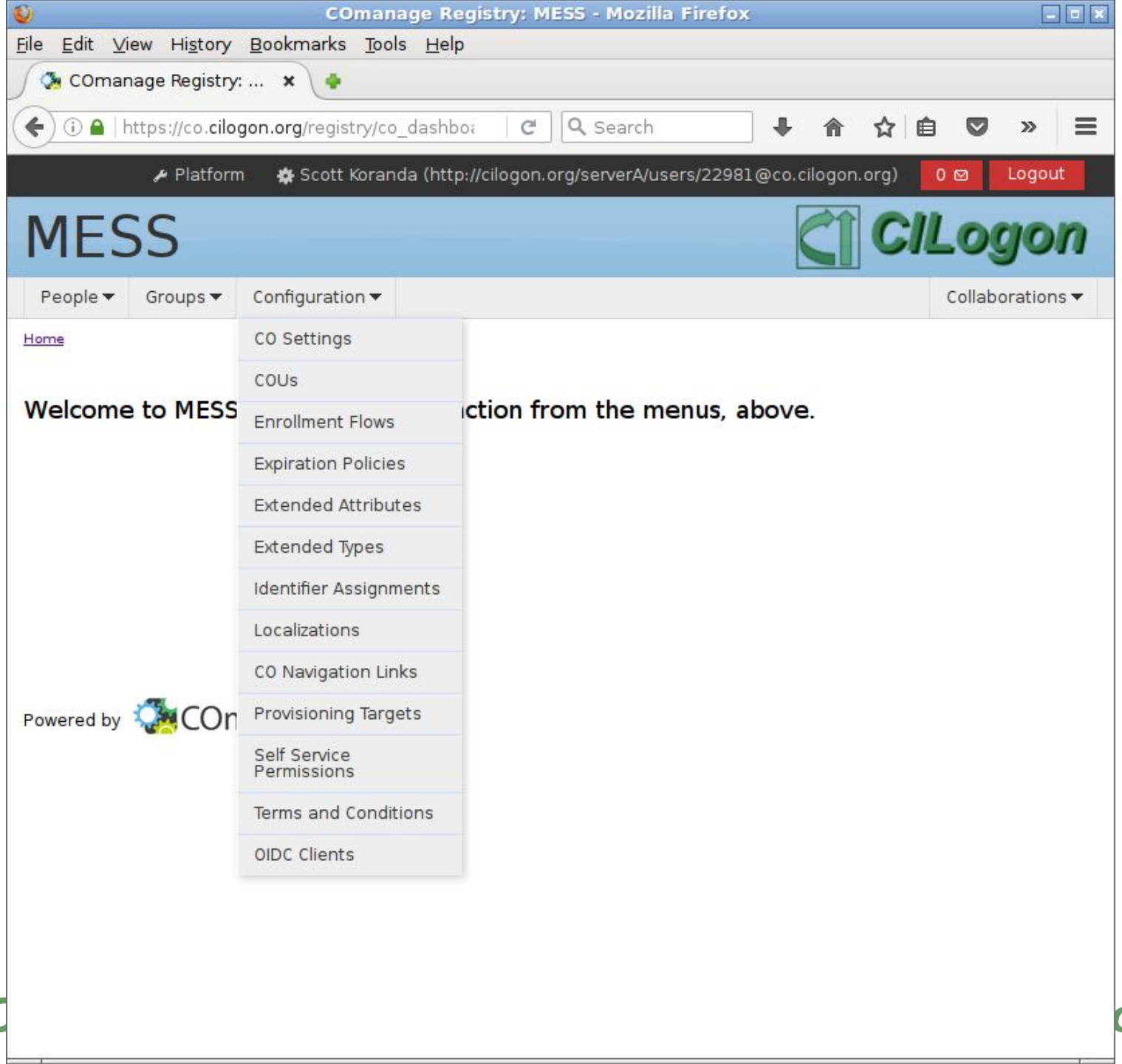
Example Walkthrough

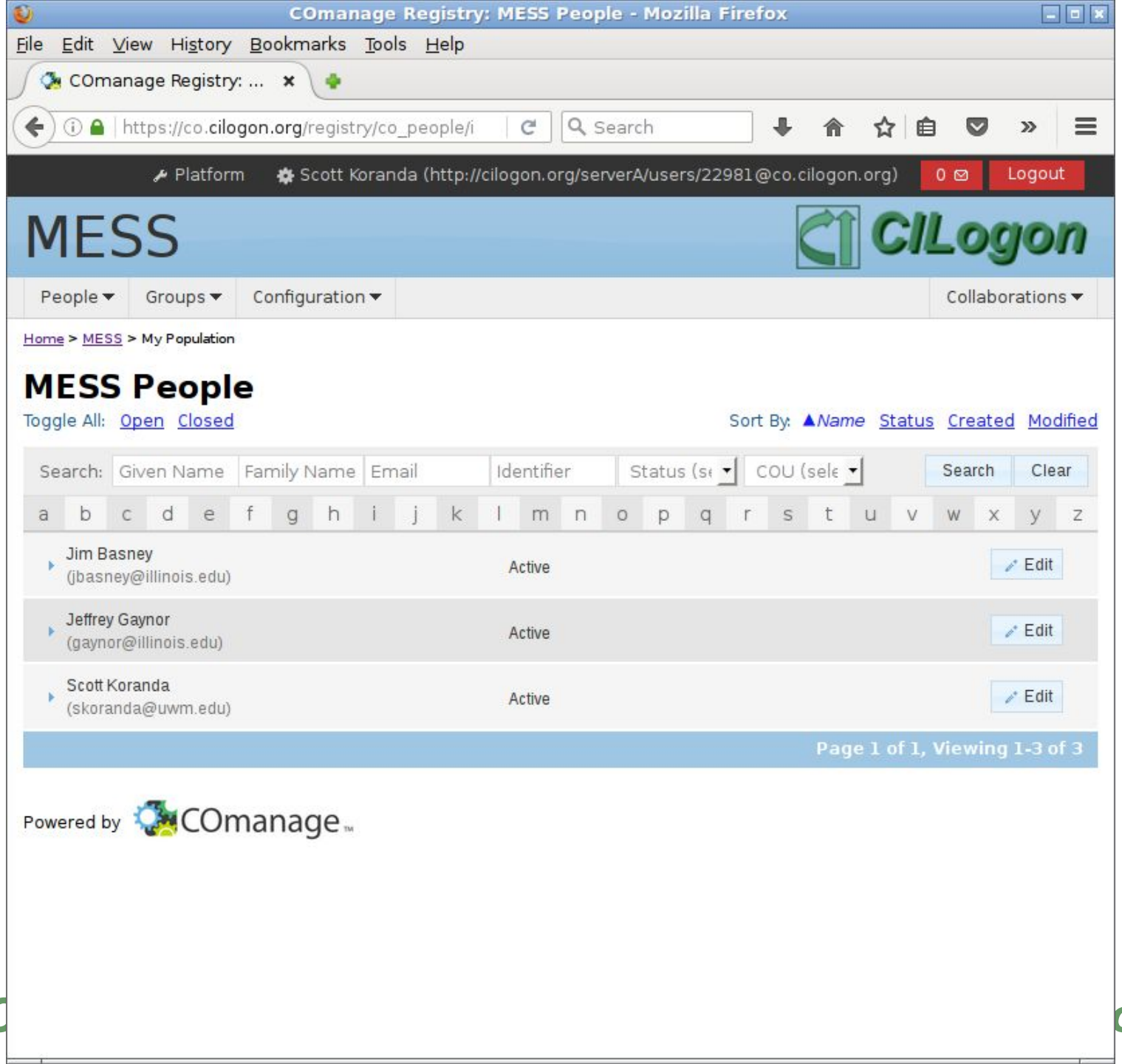
- Initial integration of CILogon OIDC with COmanage LDAP to retrieve VO memberships and ORCID iD

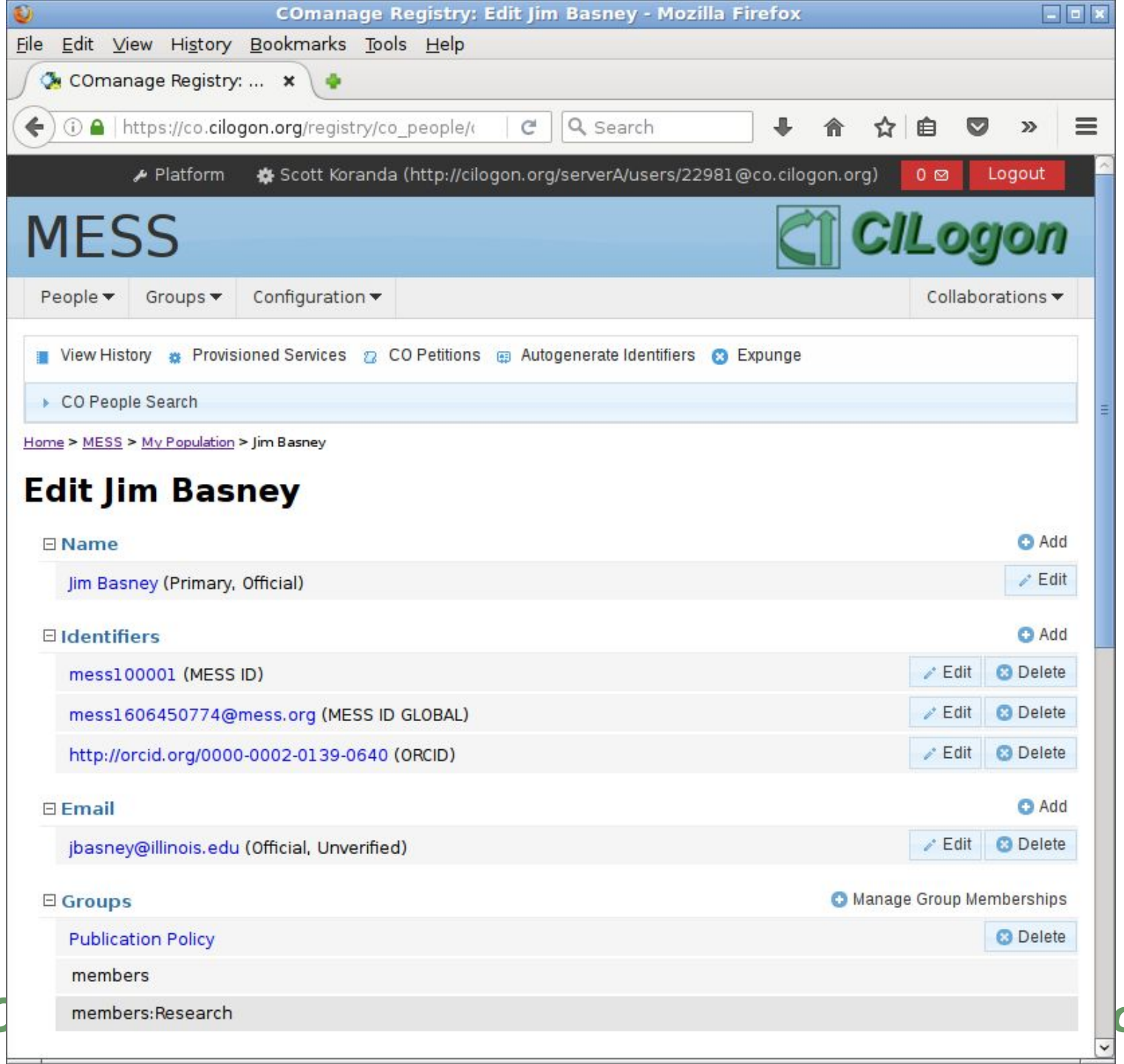


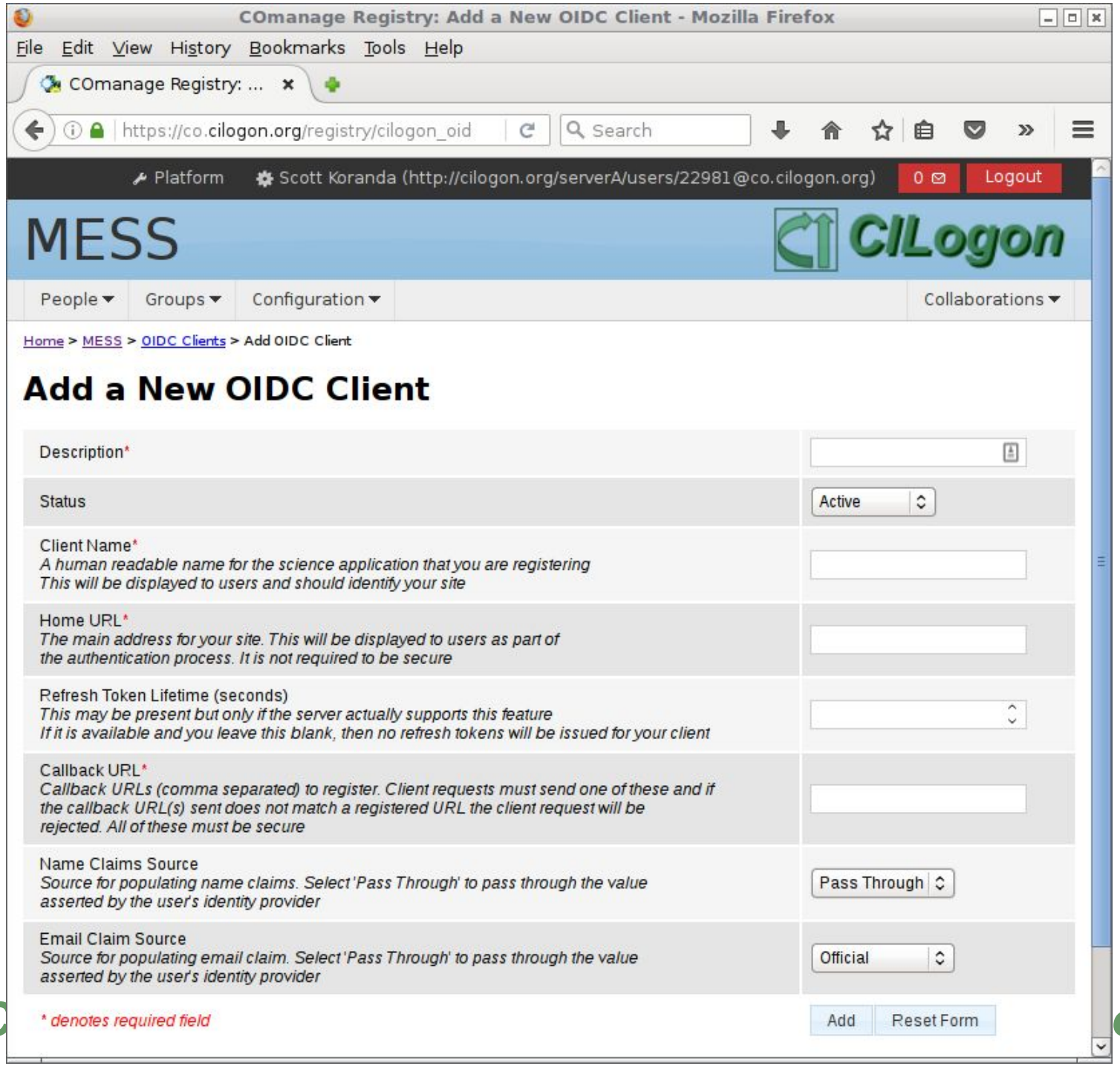

COmanage Registry: COs - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://co.cilogon.org/registry/cos
Search
Platform
Scott Koranda (http://cilogon.org/serverA/users/22981@co.cilogon.org)
Logout
COmanage Registry
CILogon
Collaborations
Home > COs
COs
Add CO
Name
Description
Status
Actions
CILogon (No VO)
CILogon user records not associated with other virtual organizations
Active
Edit
Delete
COmanage
COmanage Registry Internal CO
Active
MESS
Medium Engery Synchrotron Source
Active
Edit
Delete
Page 1 of 1, Viewing 1-3 of 3
Powered by COmanage


COmanage Registry: MESS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://co.cilogon.org/registry/co_dashboa
Search
Platform
Scott Koranda (http://cilogon.org/serverA/users/22981@co.cilogon.org)
0
Logout
MESS
CILogon
People
Groups
Configuration
Collaborations
Home
Welcome to MESS. Please select an action from the menus, above.
Powered by COmanage


COmanage Registry: MESS - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://co.cilogon.org/registry/co_dashboa
Search
Platform
Scott Koranda (http://cilogon.org/serverA/users/22981@co.cilogon.org)
0
Logout
MESS
CILogon
People
Groups
Configuration
Collaborations
Home
CO Settings
COUs
Enrollment Flows
Expiration Policies
Extended Attributes
Extended Types
Identifier Assignments
Localizations
CO Navigation Links
Provisioning Targets
Self Service Permissions
Terms and Conditions
OIDC Clients
Welcome to MESS
ction from the menus, above.
Powered by


COmanage Registry: MESS People - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://co.cilogon.org/registry/co_people/i
Search
Platform
Scott Koranda (http://cilogon.org/serverA/users/22981@co.cilogon.org)
0
Logout
MESS
CILogon
People
Groups
Configuration
Collaborations
Home > MESS > My Population
MESS People
Toggle All: Open Closed
Sort By: ▲Name Status Created Modified
Search: Given Name Family Name Email Identifier Status (se COU (sele Search Clear
a b c d e f g h i j k l m n o p q r s t u v w x y z
Jim Basney
(jbasney@illinois.edu)
Active
Edit
Jeffrey Gaynor
(gaynor@illinois.edu)
Active
Edit
Scott Koranda
(skoranda@uwm.edu)
Active
Edit
Page 1 of 1, Viewing 1-3 of 3
Powered by COmanage


COmanage Registry: Edit Jim Basney - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://co.cilogon.org/registry/co_people/
Search
Platform
Scott Koranda (http://cilogon.org/serverA/users/22981@co.cilogon.org)
0
Logout
MESS
CILogon
People
Groups
Configuration
Collaborations
View History
Provisioned Services
CO Petitions
Autogenerate Identifiers
Expunge
CO People Search
Home > MESS > My Population > Jim Basney
Edit Jim Basney
Name
Add
Jim Basney (Primary, Official)
Edit
Identifiers
Add
mess100001 (MESS ID)
Edit
Delete
mess1606450774@mess.org (MESS ID GLOBAL)
Edit
Delete
http://orcid.org/0000-0002-0139-0640 (ORCID)
Edit
Delete
Email
Add
jbasney@illinois.edu (Official, Unverified)
Edit
Delete
Groups
Manage Group Memberships
Publication Policy
Delete
members
members:Research


COmanage Registry: Add a New OIDC Client - Mozilla Firefox
File Edit View History Bookmarks Tools Help
COmanage Registry: ...
https://co.cilogon.org/registry/cilogon_oid
Search
Platform
Scott Koranda (http://cilogon.org/serverA/users/22981@co.cilogon.org)
0
Logout
MESS
CILogon
People
Groups
Configuration
Collaborations
Home > MESS > OIDC Clients > Add OIDC Client
Add a New OIDC Client
Description*
Status
Active
Client Name*
A human readable name for the science application that you are registering
This will be displayed to users and should identify your site
Home URL*
The main address for your site. This will be displayed to users as part of
the authentication process. It is not required to be secure
Refresh Token Lifetime (seconds)
This may be present but only if the server actually supports this feature
If it is available and you leave this blank, then no refresh tokens will be issued for your client
Callback URL*
Callback URLs (comma separated) to register. Client requests must send one of these and if
the callback URL(s) sent does not match a registered URL the client request will be
rejected. All of these must be secure
Name Claims Source
Source for populating name claims. Select 'Pass Through' to pass through the value
asserted by the user's identity provider
Pass Through
Email Claim Source
Source for populating email claim. Select 'Pass Through' to pass through the value
asserted by the user's identity provider
Official
* denotes required field
Add
Reset Form

OIDC JSON Response


```
{
 "sub":"http://cilogon.org/serverA/users/534",
 "name":"James Alan Basney",
 "given_name":"James",
 "family_name":"Basney",
 "email":"jbasney@illinois.edu"
 "idp_name":"University of Illinois at Urbana-Champaign",
 "idp":"urn:mace:incommon:uiuc.edu",
 "affiliation":
   "employee@illinois.edu;member@illinois.edu;staff@illinois.edu",
 "eppn":"jbasney@illinois.edu",
 "eptid":"urn:mace:incommon:uiuc.edu!https://cilogon.org/shibboleth!cyXC3O5fi0t1NB
 sW1NsOxZDyDd4=",
 "eduPersonOrcid":["http://orcid.org/0000-0002-0139-0640"],
 "isMemberOf":["members","members:Research","Publication Policy"],
 }
```

COmanage™ News

- COmanage Registry Release 2.0.0 in April 2017
- COmanage Registry Release 3.0.0 expected July 2017
  - User interface refresh
- COmanage Release 3.1 Q3 2017
  - Cluster Management, ID Match API Support, Mailing List "Native Object" Support, Enroller / Approver Attributes, Credential Management, Instrumentation and Logging, Groups as Group Members

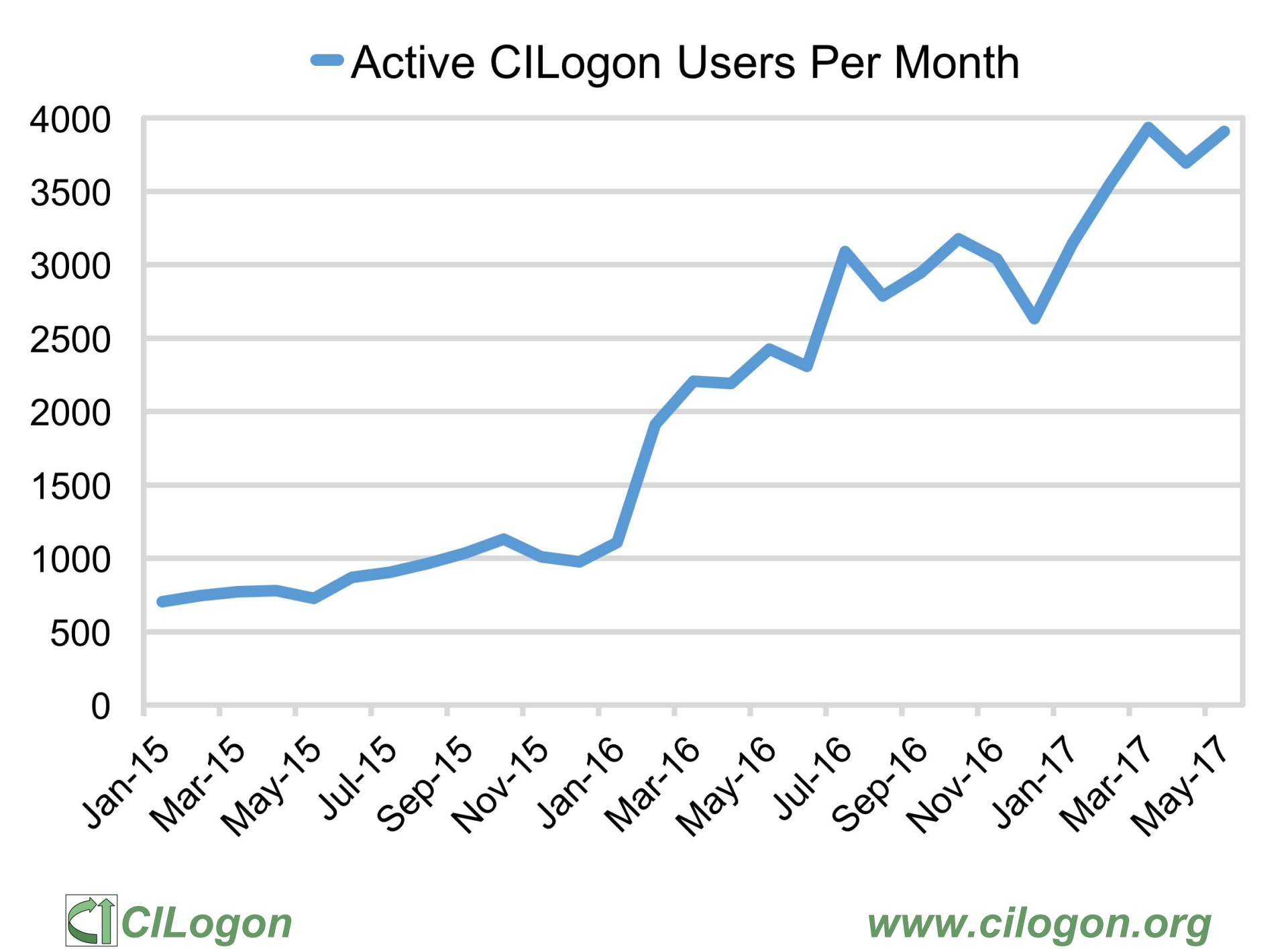
CILogon-enabled Sites

ATLAS Connect
Brandeis
Clemson
CyberGIS
CERN
CMS Connect
DataONE
DOE KBase
Duke CI Connect
Fermilab
Globus
Indiana University
LIGO
LRZ
MIT
NANOGrav (Pilot)
Northwestern
Notre Dame
OOI
OSC OnDemand
OSG Connect
SciGaP
SeedMe
SWAMP
UNL
XSEDE

Top 20 IdPs (May 2017)

FNAL
LIGO
NIH
University of Michigan
Ohio State University
Purdue University
Google
University of Chicago
UIUC
University of Minnesota
Johns Hopkins
UCLA
University of Florida
GWU
Stanford University
UC Boulder
Indiana University
UC Berkeley
LBNL
ORNL

(Out of 190 IdPs with active CILogon users)


Active CILogon Users Per Month
4000
3500
3000
2500
2000
1500
1000
500
0
Jan-15
Mar-15
May-15
Jul-15
Sep-15
Nov-15
Jan-16
Mar-16
May-16
Jul-16
Sep-16
Nov-16
Jan-17
Mar-17
May-17

CILogon 2.0 Timeline

July 2017:

- Ready for new pilot projects
- Launch of fee-based service

December 2018:

- End of CILogon 2.0 NSF grant
- Fully transitioned to sustainability model

Want to work with us?

- Research projects with collaborators across multiple institutions
- Using federated identity
- Managing group memberships and application authorization
- OAuth, OpenID Connect, SAML, LDAP, SSH, X.509
- Outsourcing IAM services
- Consistent with InCommon Research & Scholarship definition

jbasney@ncsa.illinois.edu
skoranda@sphericalcowgroup.com
info@cilogon.org