INTERNET2

2022 TECHNOLOGY exchange

Making it Sticky:
Offering Shared Services via InCommon Glue

Jim Basney
Charise Arrowood
Dedra Chamberlin
Mark Fullmer

with

Ann West
Albert Wu

Today

- Use Case: OARnet’s NSF CC* Planning Grant for **Virtual Research-Education Ohio (VROhio)**
- Solution: Digital IAM swiss army knife from Cirrus Identity
- Solution: Federation Gateway from Unicon
- Solution: CILogon
- Q&A

Introduction - The Panel

Jim Basney

Charise Arrowood

Dedra Chamberlin

Mark Fullmer

Today’s Goals

OARnet

NSF CC* Planning Grant As A Use Case

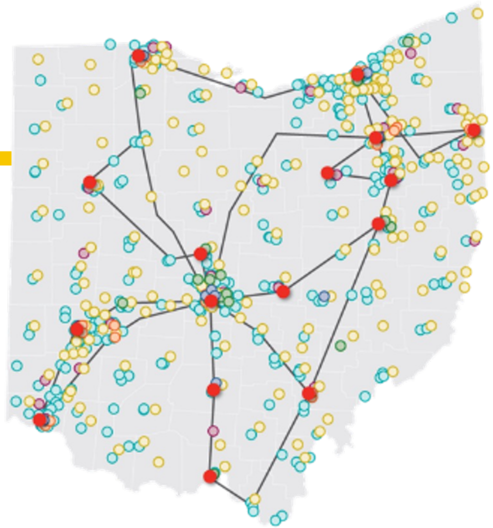
Making Federation Sticky

OARnet NSF CC* Planning Grant As A Use Case

Mark Fullmer, OARnet Chief Technology Officer

OARnet Communities

Serving



2879

State gov't sites

48 State Agencies

98

Local Entity sites

63 clients

102

Healthcare sites

7 clients

625+

K-12 Schools

600+ school districts

469

Higher Education

100 main campuses

324 regional campuses

27

Public Broadcasting

10 stations

13

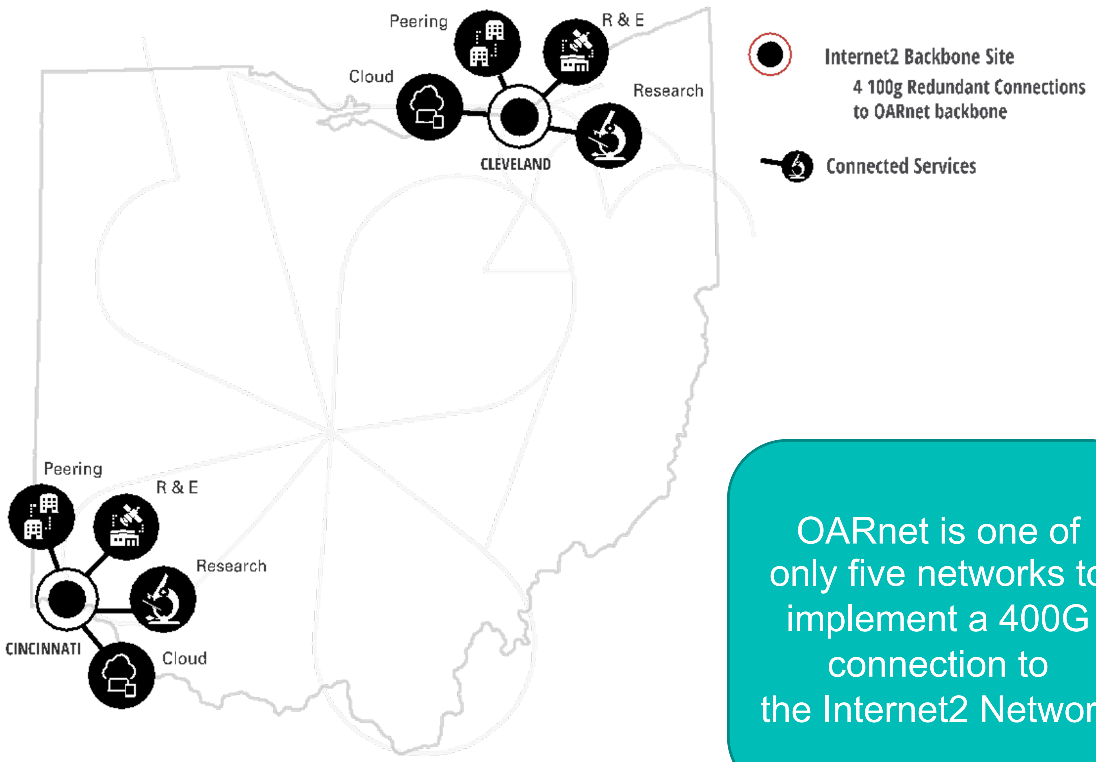
Research sites

8 clients

ESInet
Service Provider

Supporting NG-911 services for 9 counties, 4 cities and 1 university with future sites planned.

Internet2 400G Circuits



4x100G in Cleveland

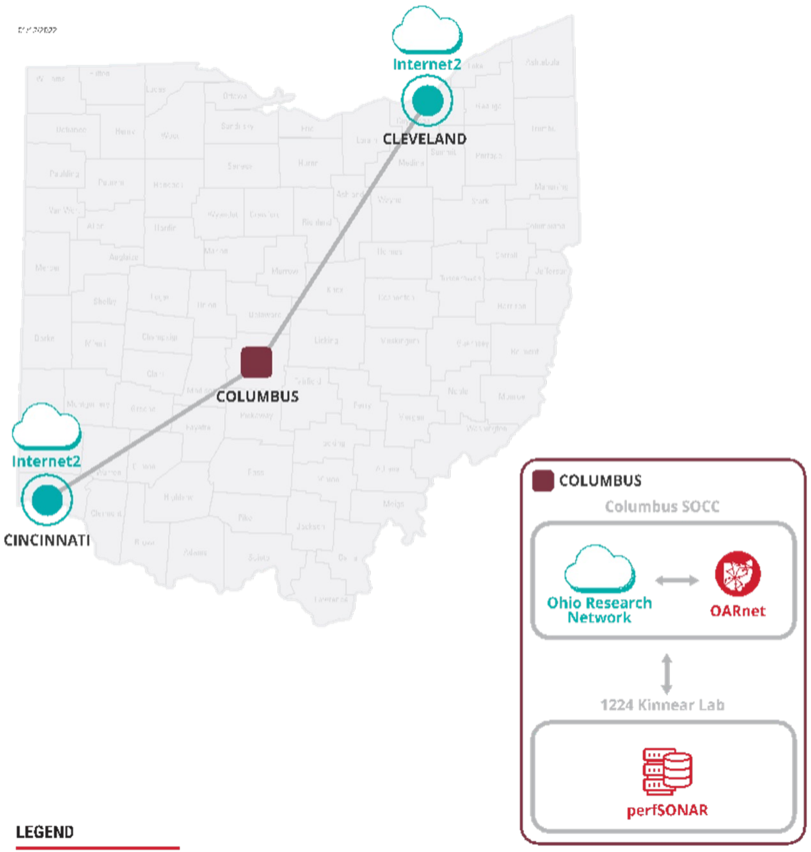
- Commercial Peering
- R&E Network
- Cloud Computing
- Research projects (non-production)

OARnet is one of only five networks to implement a 400G connection to the Internet2 Network

4x100G in Cincinnati

- Commercial Peering
- R&E Network
- Cloud Computing
- Research projects (non-production)

OARnet 100g Research Infrastructure



LEGEND

100g OARnet Backbone

CC* Planning: Virtual Research-Education Ohio (VROhio)
PI: Pankaj Shah | Co-PI: Mark Fullmer
Proposal #: 2126199

Objectives:

1. Identify network-enabled education, training and research applications and their requirements
2. Chart a course toward a statewide federated identity management system and DMZ/VPN network segments for sharing educational and research services
3. Build a working group to identify and encourage the development and adoption of shareable resources needed by under-resourced higher education institutions (HEIs)
4. Prepare proposals to the NSF CC* program or other programs to fund these activities
5. Strengthen capabilities that enhance the high school to higher education STEM pipeline (e.g. the Ohio College Credit Plus Program)

Participating Colleges:

- Chatfield College
- Columbus State Community College
- Franciscan University of Steubenville
- Lorain County Community College
- Malone University
- Northwest State Community College
- Sinclair Community College
- Terra State Community College
- Xavier University

Collaborators:

- Engagement and Performance Operations Center (EPOC)
- InCommon/Internet2
- Ohio Supercomputer Center (OSC)
- OhioLINK *identified during planning
- Case Western Reserve University (CWRU)
- The Quilt
- Trusted CI

Deliverables:

- Development of OARnet virtual research and education DMZ network and associated services:
  - Design of federated identity management services for the DMZ network and end user services
  - Design VPN access service to the DMZ network for off-campus remote access
  - Engage with Trusted CI for security design review
  - Establish functions and job descriptions for CI application experts
  - Determine optimum placement of perfSONAR and DTN
- Institution and faculty services design
  - Build a community of practice within the OARnet member HEI consisting of faculty, network engineers and CI experts engaged in identifying and developing shared teaching and research applications
  - Design a process for developing shared applications as production quality shared services including proposing new services, gathering and analyzing requirements, prototyping, testing and production rollout.
  - Educate participants about using InCommon for authentication and Trusted CI program

Federated identity goals

- Review high-level functions of Identity and Access Management and how to integrate InCommon federation
- Learn how to leverage InCommon to enable federated access to academic collaborations in Ohio and throughout Higher Education
- Identify available options to connect to InCommon and the IAM community

Ohio InCommon Community Members

- Case Western Reserve University
- John Carroll University
- Kent State University – Main Campus
- Miami University
- The Ohio State University
- University of Akron – Main Campus
- University of Cincinnati – Main Campus
- University of Dayton
- University of Toledo

Community member backgrounds

- Research
- Teaching & Learning
- Systems Engineers
- Network Engineers
- Cybersecurity
- OARnet staff including administrative management, client services, network engineering, systems, and security

Candidates for federated identity projects

1. Case Western Reserve University Electron Microscope lab
2. Ohio Supercomputer center compute and storage facilities
3. Kent State University research lab
4. OhioLINK library consortia

Identity Management implementation survey results

- Baldwin Wallace – Azure AD
- Case Western Reserve University – Shibb, SAML, Kerberos, AD, LDAP
- Chatfield College – Canvas
- Lorain Community College – Azure AD; Microsoft ADFS
- Malone University – Locally developed, migrating to Azure AD
- Sinclair Community College – Azure AD
- Terra State Community College – Microsoft ADFS
- Xavier University – Azure AD, SAML

InCommon Virtual Engagement BaseCamp

1. Discuss level of interest and potential objectives for future participation in the program. Identify key collaborators
   - Ohio Supercomputing center (OSC)
   - OhioLink (statewide library system)
2. Essential functions of identity and access management in a Higher Education organization
3. Basics of federation with focus on how trust is built through policy, process, and community
4. Technical solutions presented by InCommon and their Catalyst partners

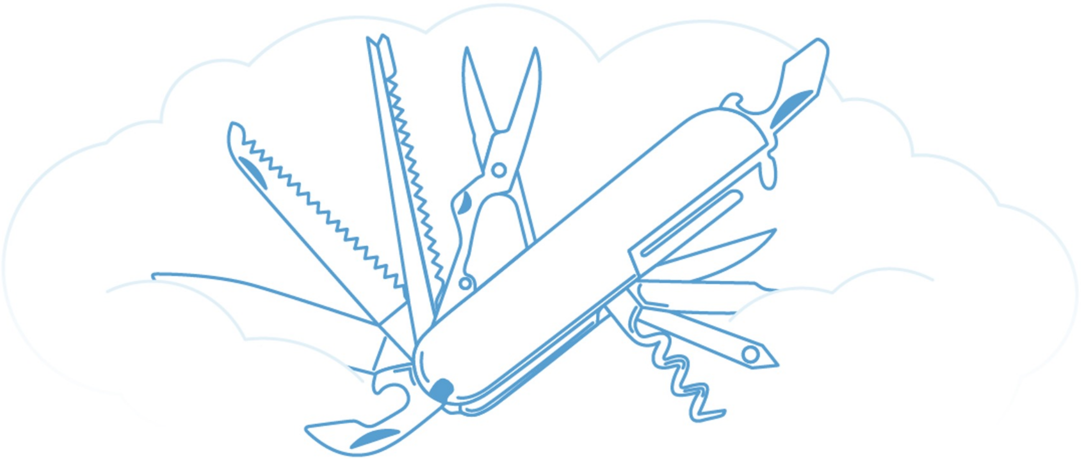
Key Outcomes

1. Explore solutions to enable federation
    1. Aggregate purchasing agreements for Gateway/Bridge software
    2. Use of separate state-wide identity provider which could be shared among small and medium sized institutions in Ohio
    3. Using InCommon as a Federation framework using an aggregate purchasing model
2. Significant effort will be required to enable Ohio R&E institutions to offer, utilize, and benefit from Federated identity services.
    1. Lower the barrier to entry with aggregate purchasing
    2. Create a pool of cyberinfrastructure engineers within OARnet
3. Create a non-production 100G infrastructure in Ohio connected to Internet2 for experimental services (not limited to Federated Identity initiative)

Next steps…

cirrus identity

Your Swiss Army Knife for Digital Identity Management



Cirrus Identity is a Trusted InCommon Catalyst Partner

InCommon/eduGAIN Trust

Value for Identity Providers

Streamline and Expand Access for your Users

Challenge:

Popular Commercial IAM solutions Don’t Support Multilateral Federation

Azure Active Directory okta Google Workspace DUO

Solutions:

Shibboleth – InCommon Trusted Access Platform

SimpleSAMLphp – Popular Open Source Project

Cirrus Bridge – Hosted multilateral federation

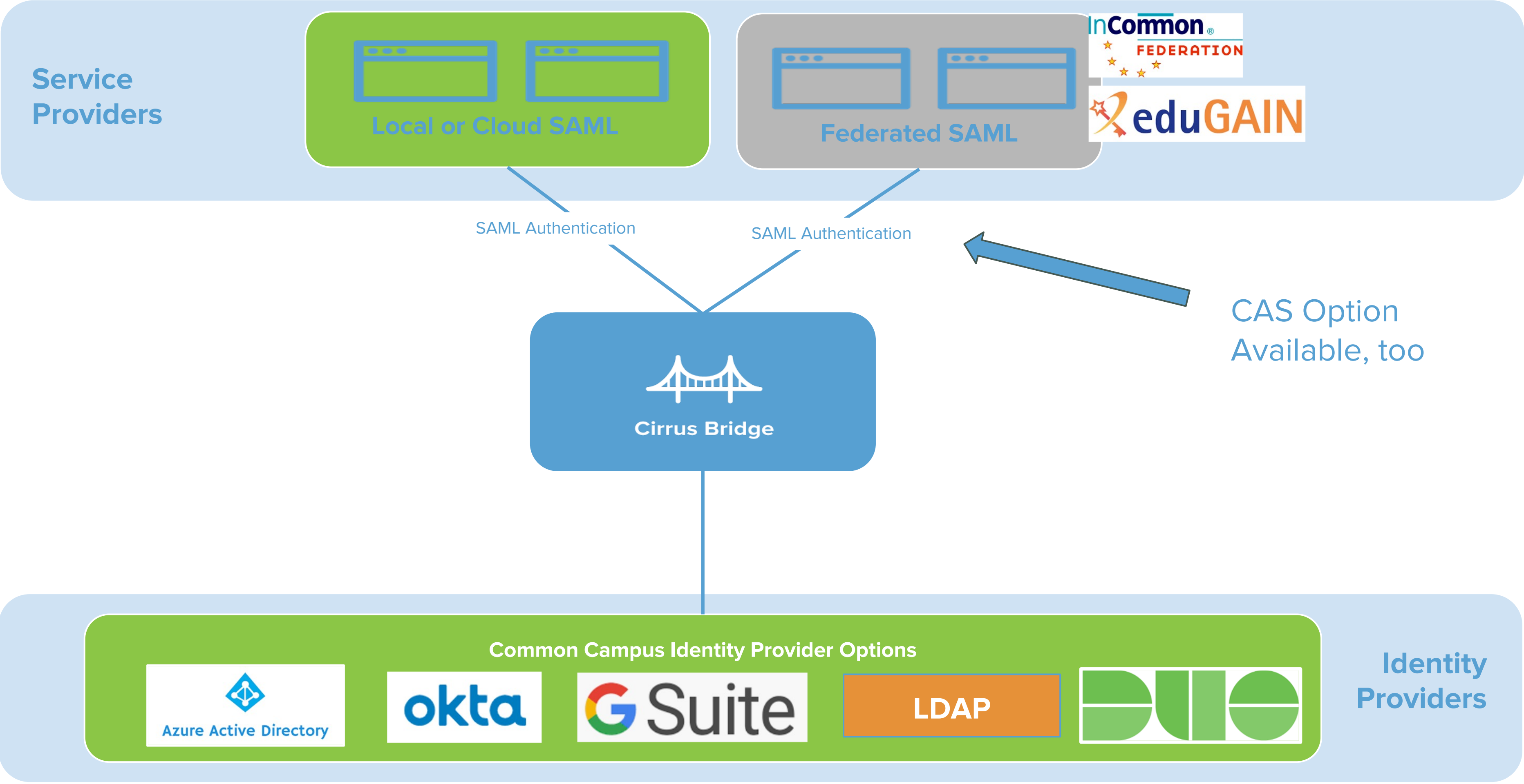
”bridge” for Azure AD, Okta, DUO SSO, Google Workspace and more

Shibboleth.

simpleSAMLphp

Cirrus Bridge

Connect your Campus IdP to InCommon/EduGAIN



Service Providers

Local or Cloud SAML

Federated SAML

InCommon FEDERATION

eduGAIN

SAML Authentication

SAML Authentication

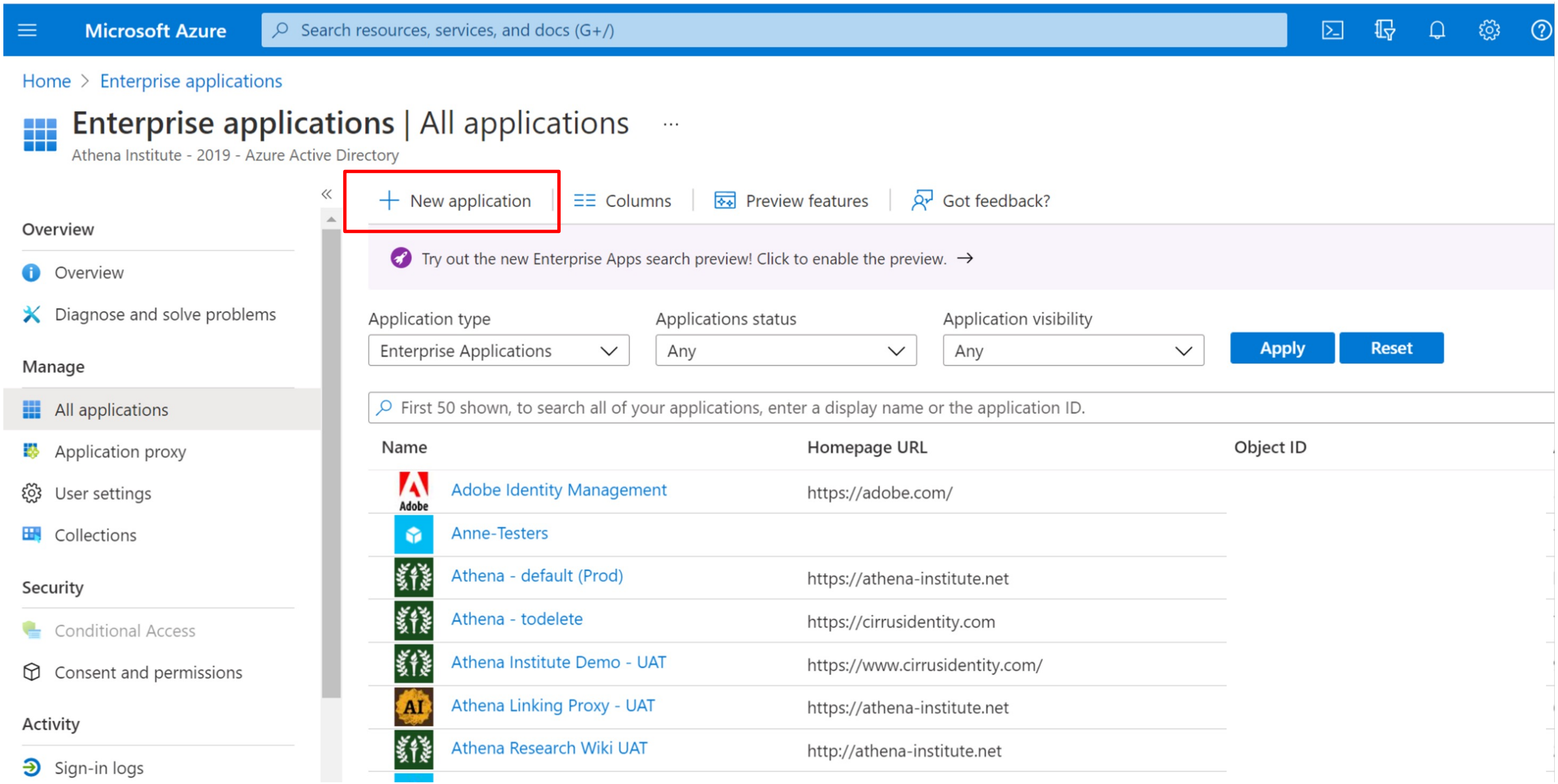
CAS Option Available, too

Cirrus Bridge

Common Campus Identity Provider Options

Identity Providers

Almost all the configuration happens in the Azure AD, Okta, DUO SSO Portal



Enterprise applications | All applications

Athena Institute - 2019 - Azure Active Directory

Try out the new Enterprise Apps search preview! Click to enable the preview. →

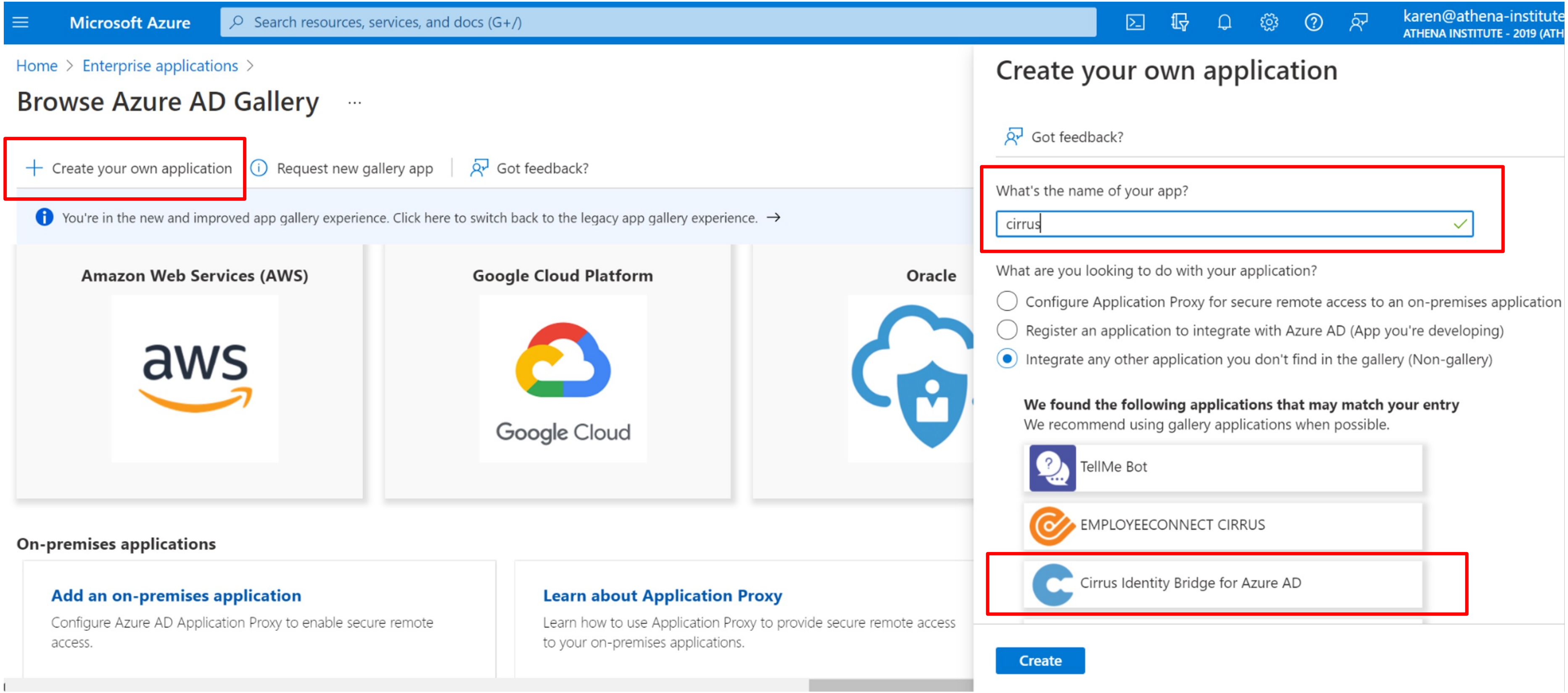
Application type: Enterprise Applications

Applications status: Any

Application visibility: Any

First 50 shown, to search all of your applications, enter a display name or the application ID.

Name	Homepage URL	Object ID
Adobe Identity Management	https://adobe.com/	
Anne-Testers		
Athena - default (Prod)	https://athena-institute.net	
Athena - todelete	https://cirrusidentity.com	
Athena Institute Demo - UAT	https://www.cirrusidentity.com/	
Athena Linking Proxy - UAT	https://athena-institute.net	
Athena Research Wiki UAT	http://athena-institute.net	



Microsoft Azure

Search resources, services, and docs (G+/)

karen@athena-institute

ATHENA INSTITUTE - 2019 (ATH

Home > Enterprise applications >

Browse Azure AD Gallery ...

+ Create your own application | ⓘ Request new gallery app | Got feedback?

ⓘ You're in the new and improved app gallery experience. Click here to switch back to the legacy app gallery experience. →

On-premises applications

Add an on-premises application

Configure Azure AD Application Proxy to enable secure remote access.

Learn about Application Proxy

Learn how to use Application Proxy to provide secure remote access to your on-premises applications.

Create your own application

Got feedback?

What's the name of your app?

cirrus ✓

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application

○ Register an application to integrate with Azure AD (App you're developing)

● Integrate any other application you don't find in the gallery (Non-gallery)

We found the following applications that may match your entry

We recommend using gallery applications when possible.

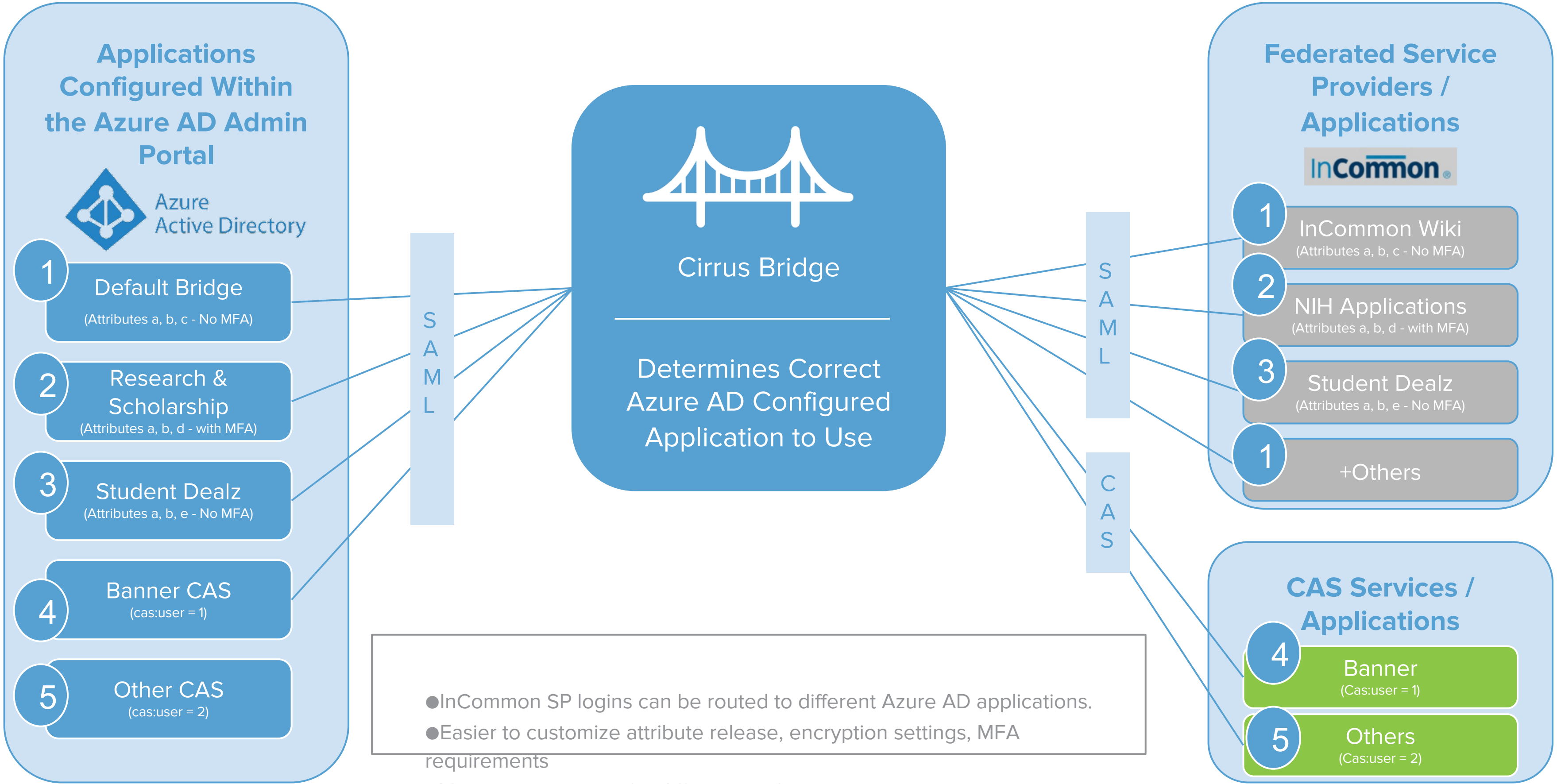
- TellMe Bot
- EMPLOYEECONNECT CIRRUS
- Cirrus Identity Bridge for Azure AD

Create

The Cirrus Bridge Supports:

- Azure AD/Okta Conditional Access
- REFEDS Research and Scholarship Categories
- REFEDS MFA Authentication Context

Bridge Conditional Access Configuration - Azure AD Portal



Applications Configured Within the Azure AD Admin Portal
Azure Active Directory
1 Default Bridge (Attributes a, b, c - No MFA)
2 Research & Scholarship (Attributes a, b, d - with MFA)
3 Student Dealz (Attributes a, b, e - No MFA)
4 Banner CAS (cas:user = 1)
5 Other CAS (cas:user = 2)
SAML
Cirrus Bridge
Determines Correct Azure AD Configured Application to Use
SAML
CAS
Federated Service Providers / Applications
InCommon
1 InCommon Wiki (Attributes a, b, c - No MFA)
2 NIH Applications (Attributes a, b, d - with MFA)
3 Student Dealz (Attributes a, b, e - No MFA)
1 +Others
CAS Services / Applications
4 Banner (Cas:user = 1)
5 Others (Cas:user = 2)

- InCommon SP logins can be routed to different Azure AD applications.
- Easier to customize attribute release, encryption settings, MFA requirements
- View metrics usage for different applications

Making it easier to expand the InCommon/eduGAIN trust framework

- We work with statewide systems and grant-funded research projects that need to onboard many organizations to federation
- Discounted bulk pricing available for consortium and systems that need 3 Bridges or more
- Can streamline collaboration between organizations with heterogeneous IAM systems (some on Azure AD, some on DUO SSO, some on Okta)

InCommon/eduGAIN Trust

Value for Service Providers

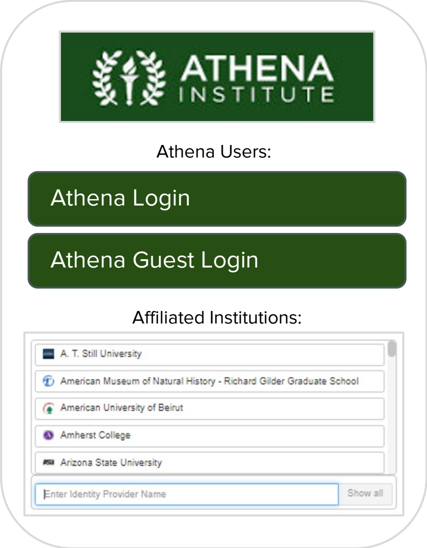
Quickly and easily Integrate with InCommon/eduGAIN Identity Providers

The Cirrus Proxy Includes:

- Integration with InCommon/eduGAIN IdPs
- Easily configurable discovery service
- Option to add:
  - OrgBrandedID as IdP of Last Resort for guests
  - Invitation service for sponsored accounts
  - Account linking service

Customer Login Discovery Concept

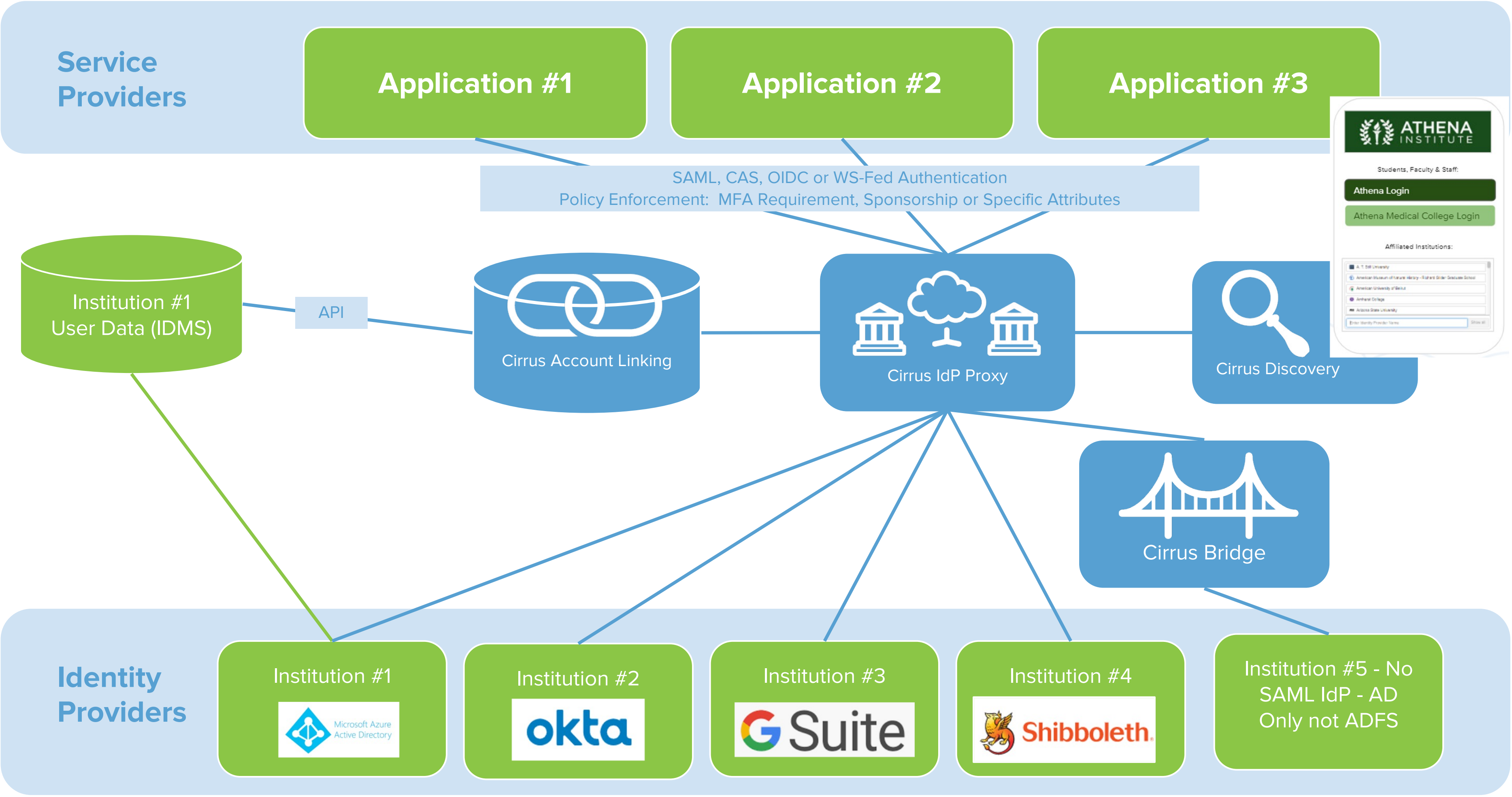
Conceptual login discovery screen available for applications that require users from multiple institutions



Takes users to institution’s primary identity provider

Scrolling or configure buttons for affiliated institutions so users can use their own username & password to access applications

Cirrus Proxy Solution Architecture



ATHENA INSTITUTE

Students, Faculty & Staff:

Athena Login

Athena Medical College Login

Affiliated Institutions:

A. T. Still University

American Museum of Natural History - Richard Gilder Graduate School

American University of Beirut

Amherst College

Arizona State University

Enter Identity Provider Name

Show all

For more information:

https://cirrusidentity.com

sales@cirrusidentity.com

UNICON®

- Unicon is a technology consulting firm focused solely on the education ecosystem
- We partner with institutions and companies to create learner-centric digital experiences to transform online teaching and learning.
- We believe in the power of technology to expand access to education, and in the power of education to create a better future for all.
- Unicon is an AWS Partner Network (APN) Advanced Consulting Partner, has achieved the AWS Education Competency, and is a member of the AWS Public Sector Partner Program.

Let's "Make it Sticky" together!

Federation Gateway Benefits

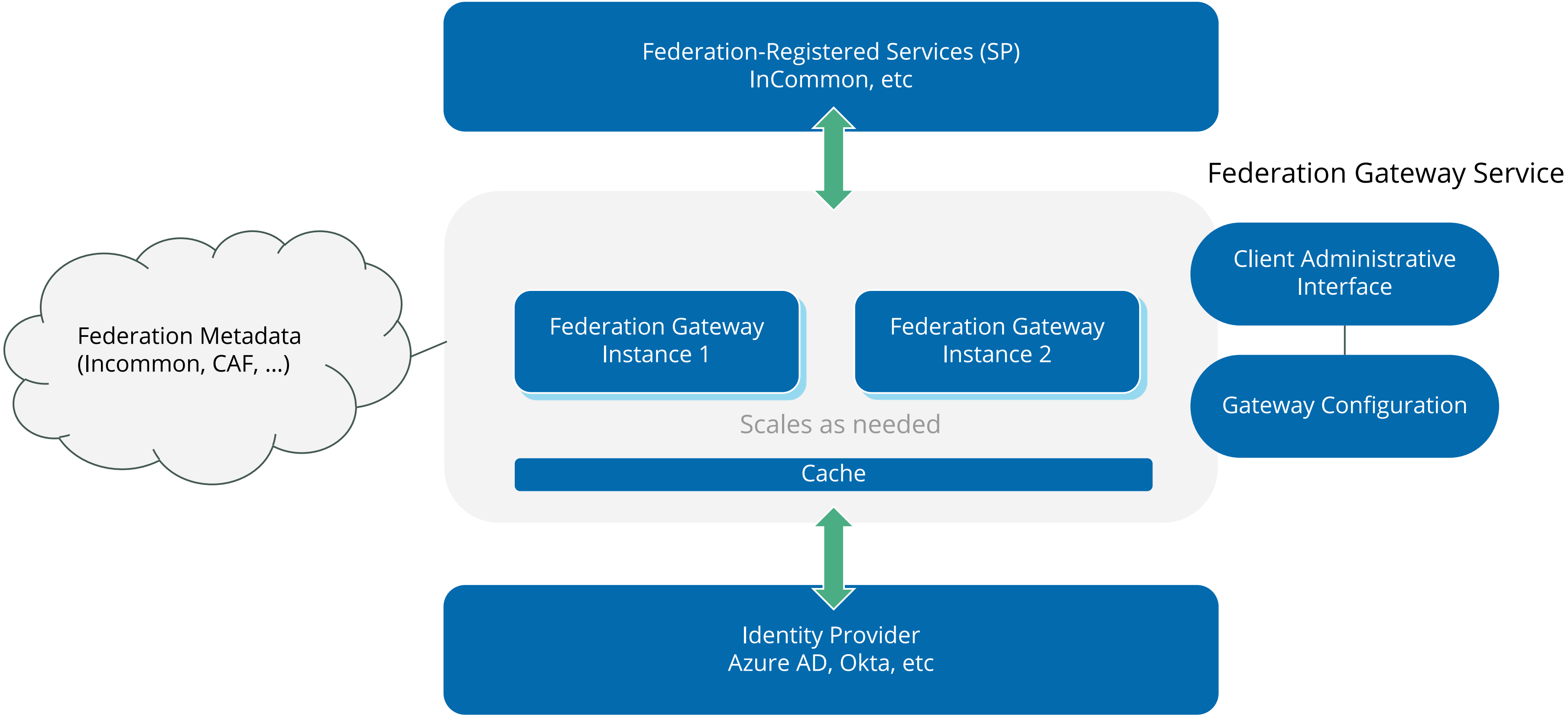
- Using the Federation Gateway, you can easily connect to the identity federation of your choice, allowing seamless set-up of participating SPs—you no longer have to add each SP individually.

- You can choose from a variety of attribute release policies, including releasing all attributes, releasing no attributes, and allowing the end-user to choose which attributes to release.

- The Federation Gateway is hosted in AWS and uses AWS technology to provide redundancy and scalability.

- Unicon can share expertise to help your organization manage and maintain the Federation Gateway in your environment.

Unicon - Federation Gateway



Federation-Registered Services (SP)
InCommon, etc

Federation Gateway Service

Federation Metadata
(Incommon, CAF, ...)

Federation Gateway
Instance 1

Federation Gateway
Instance 2

Scales as needed

Cache

Client Administrative
Interface

Gateway Configuration

Identity Provider
Azure AD, Okta, etc

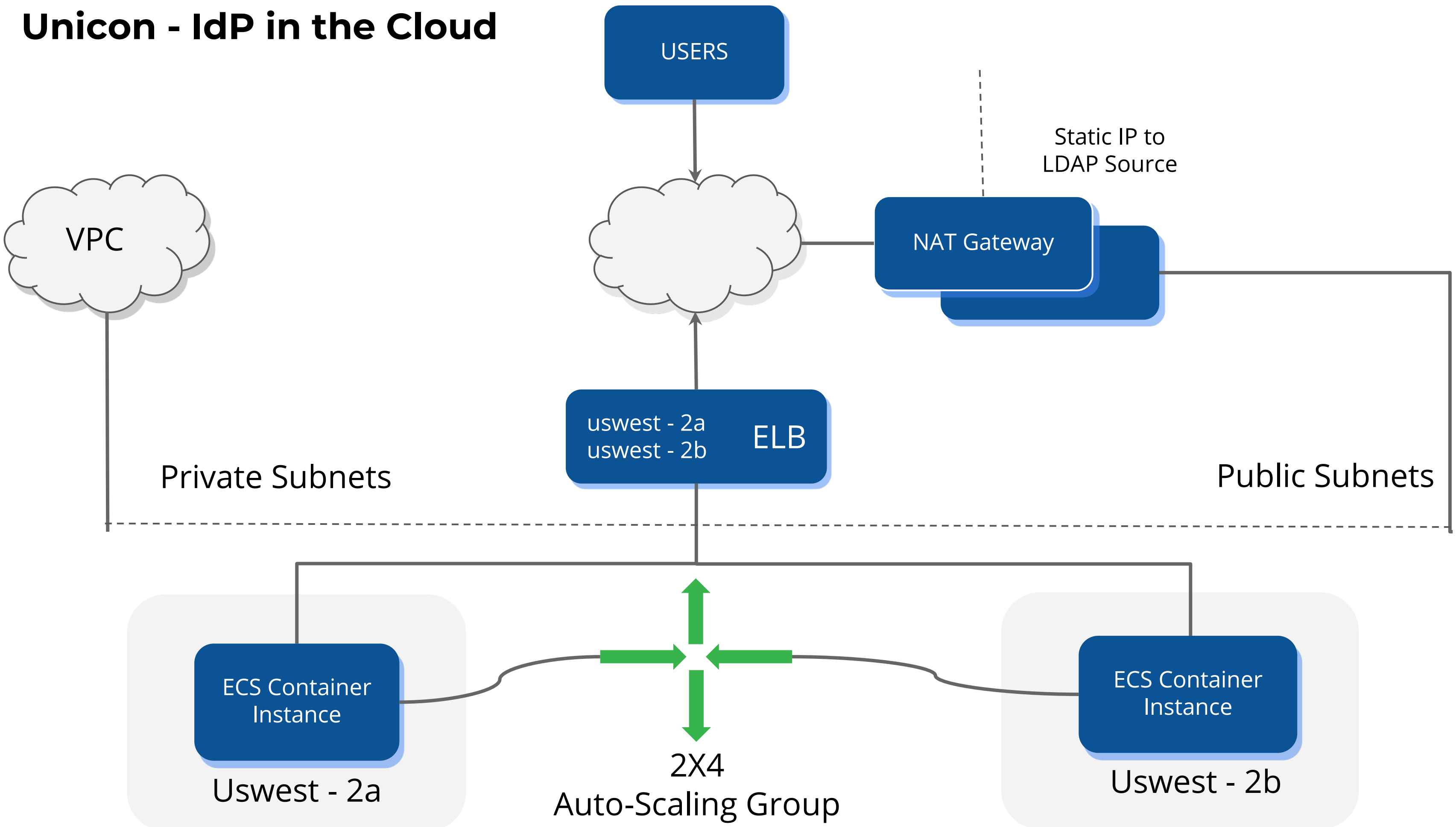
IdP in the Cloud Benefits

- Federated Web SSO in the Cloud
- Fully managed, full featured hosted IdP
- Unicon does the work so you don't have to!

Includes:

- Duo Security-based MFA
- Encrypted authentication responses
- LDAP-based authentication
- LDAP-based attribute resolution
- Logout - possible
- Signed Authentication Request
- Single Logout (SLO) - possible with caveats
- SAML 2 Browser SSO (HTTP-Redirect, HTTP-POST) Profile

Unicon - IdP in the Cloud



UNICON®

Custom Fully Managed Greenfield Opportunities in the Cloud

References implementations, already built and managed

- Statewide K-12 system in Midwest
- West coast community college system
- EdTech custom proxy

Unicon will collaborate with you and recommend the technology and path to meet your hosting and managed services needs.

Mike Grady
mgrady@unicon.net

Charise Arrowood
carrowood@unicon.net

UNICON®

CILogon

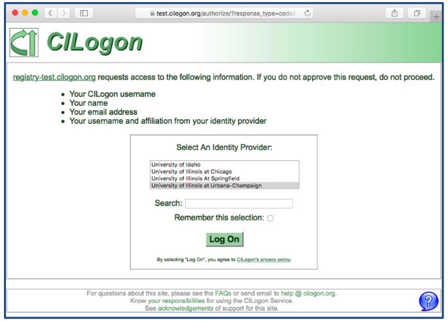
10+ year sustained effort to enable secure logon to scientific cyberinfrastructure (CI)

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 20,000+ active users from 500+ organizations around the world

with onboarding/offboarding/attributes/groups/roles managed consistently across multiple applications



registry-test.cilogon.org 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

Select An Identity Provider:

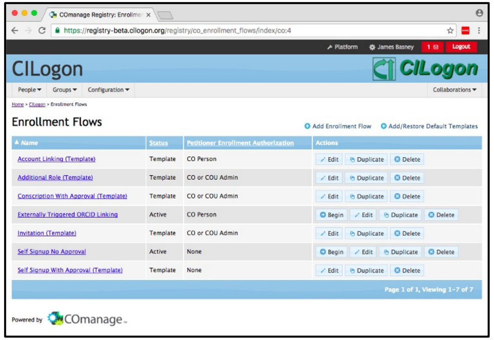
University of Idaho
University of Illinois at Chicago
University of Illinois At Springfield
University of Illinois at Urbana-Champaign

Search:

Remember this selection: □

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.


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

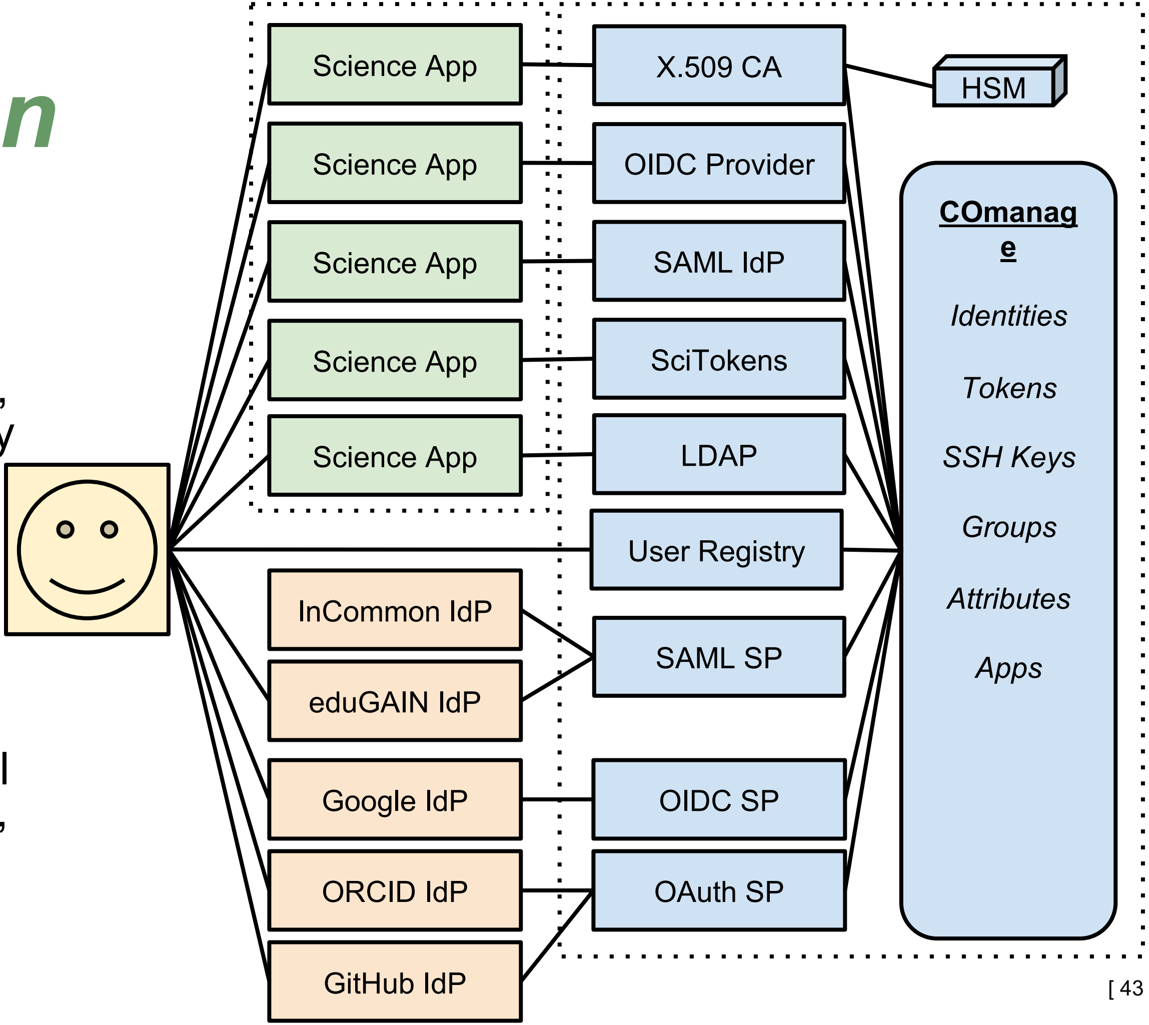
Name	Status	Petitioner Enrollment Authorization	Actions
Account Linking (Template)	Template	CO Person	Edit Duplicate Delete
Additional Role (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Conscription With Approval (Template)	Template	CO or COU Admin	Edit Duplicate Delete
Externally Triggered 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

CILogon

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, GitHub, Microsoft, ORCID)



Science App

Science App

Science App

Science App

Science App

X.509 CA

HSM

OIDC Provider

SAML IdP

SciTokens

LDAP

User Registry

InCommon IdP

eduGAIN IdP

SAML SP

Google IdP

OIDC SP

ORCID IdP

OAuth SP

GitHub IdP

COmanag
e

Identities

Tokens

SSH Keys

Groups

Attributes

Apps

CILogon

example integrations

2i2c, ACCESS, Apache Airavata Test Drive, Ask.CI, ATLAS Connect, Australian BioCommons, BNL Quantum Astrometry, Brainlife.io, CADRE,
CERN PanDA, Chem Compute, ClassTranscribe, CloudBank, Clowder,
CMS Connect, Connect.ci, Custos, CyberGISX, CyVerse, DataCite, Duke CI Connect, Einstein Toolkit, FABRIC, Fermilab, Flywheel, GeoChemSim, Globus, GW-Astronomy, HubICL, HTRC, ImPACT, LIGO, LROSE, LS-CAT, LSST, Mass Open Cloud, MIT Engaging OnDemand, MSU HPCC OnDemand, MyGeoHub, NCAR PRESTO, NEON, NIH ClinOmics, NIH KnowEnG,
Ocean Observatories Initiative, Open Science Chain, OSC OnDemand,
OSG Connect, Pacific Research Platform, QUBES, SciGaP, SCiMMA

CILogon

for more info:

jbasney@cilogon.org
info@cilogon.org

https://www.cilogon.org/subscribe

End of Presentation Deck

Materials beyond this point are for working notes / background. They are not part of the presentation deck.

Session Abstract

Have services you want to offer schools in your state or region, but it’s tough to manage the individual access details? Want to help your member campuses access those shared services and the world of academic collaboration? The community has news for you!

Learn about a recent OARnet’s experience and how the community has been working on several initiatives to help a diversity of organizations to participate. There are also education programs and partner-provided tools to help bridge the gap. Please join the panel and explore resources available to support your needs.

Possible Flow

Goal

- Attendees hear from a consortium/state-based organization about how they plan to use InCommon to serve local needs.
- Attendees leave with information on how to find out more and host SP and IdP infrastructure

Ann or Albert - MC - Intro the speakers - 5 min

Mark – 15 min

- presents the OARnet use case about receiving NSF funding to bring in a diverse set of schools into InCommon to share services and collaborate. They want to support both idP and Sps, but how do they do that without each organization running their own federation software? Hosting options!

Hosted IdPs

- Cirrus – 10 min
- Unicon – 10 min

Hosted identity infrastructure for SPs

- CI Logon – 10 min

Closing with mention of InCommon Good housekeeping Seal Program

- Maybe have time for one question…

Questions to ask/address