U.S. ARF / CICoE Pilot / Trusted CI Identity Management (IdM) Engagement

John Haverlack
R/V Sikuliaq
College of Fisheries and Ocean Sciences
University of Alaska Fairbanks

Josh Drake
Ci CoE Pilot/Trusted CI
Indiana University Center for Applied Cybersecurity Research

Ryan Kiser
Trusted CI
Indiana University Center for Applied Cybersecurity Research

CI CoE PILOT

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CILogon

COmanage™

ARF IdM Engagement Plan

https://docs.google.com/document/d/1Btb4VRaXrZzg_8brZ_viSMy20PNH-AlcTnamwwr22Ss/edit

May - October 2020

- **Milestone 1:** Catalog Current State of IdM in the ARF
- **Milestone 2:** Recommend an IdM solution
- **Milestone 3:** Proof of concept IdM solution

Objectives of a Federated IdM Service

This engagement explored how to:

- Provide an Opt-In per vessel per service IdM Solution
- Centralized Identity Management capability for the Fleet
- Facilitate Auditability of Authentication Events
- Monitor expired or inactive accounts for deactivation
- Reduce use of shared password accounts
- Leverage Institutional Identity Providers rather than creating new identities
- Streamline On/Off Boarding Processes
- Develop a Shipside Authentication Appliance

IdM Primer Video

IdM Primer Video
https://youtu.be/rZWOXeOsN6E

IdM Primer Presentation
https://docs.google.com/presentation/d/1_riLUbkQYiqvOsPXezn3GLwehj1WEWLwfiELo4qwxiE/edit?usp=sharing

- Authentication
- Authorization
- Authentication Services
- Auditability
- Shared Accounts
- Federated Identity Services

Milestone 1: State of IdM in US ARF - Survey Results

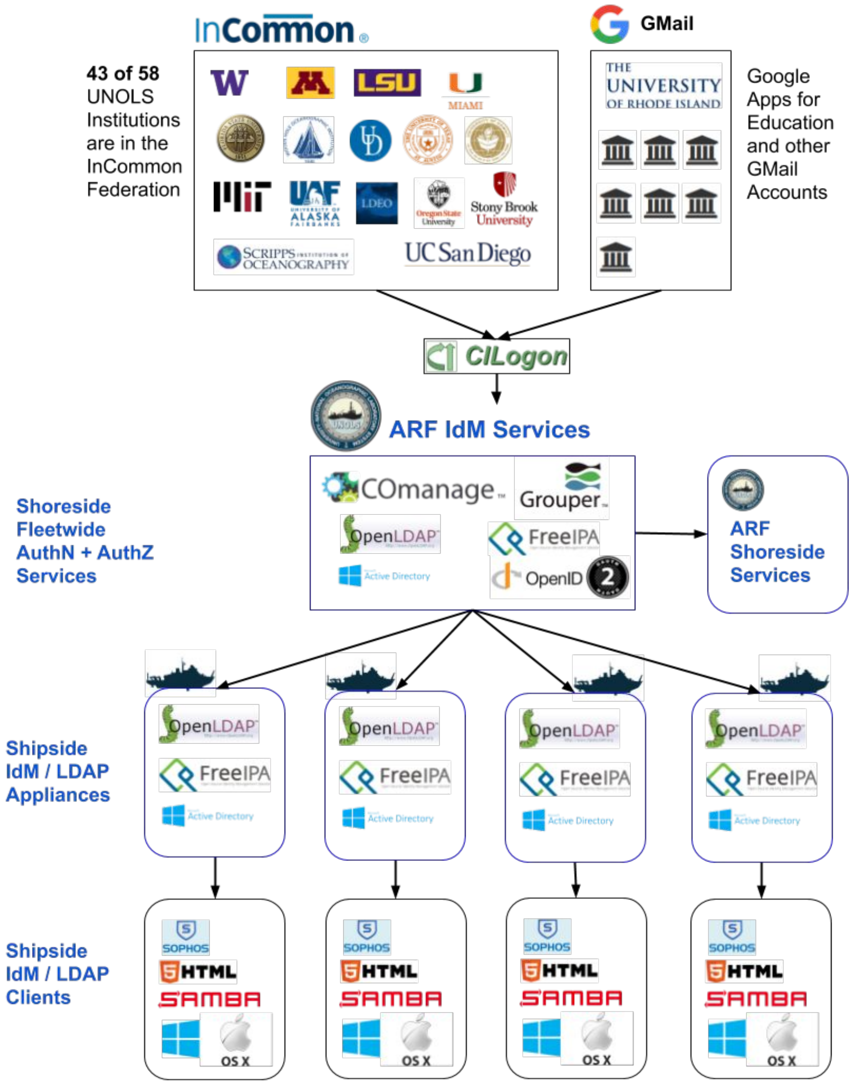
- 10 Institution Responded / 15 Vessels Represented
- 60% don’t know how many Institute accounts are accessed each year
- 50% don’t know how many Transient accounts are accessed each year
- 80% don’t know how many inactive accounts are enabled
- Shared Password Roll Accounts are commonly used
- Majority of Credentials are managed locally on each device
- A small number of vessels use AD/LDAP
- End users are storing passwords insecurely
- 60% have only local system logs / 20% have centralized logging
- 10% regularly audit logs
- Majority require strong passwords / 30% use 2FA
- There is a mix of processes for adding / removing accounts

Milestone 1: State of IdM in US ARF

Survey Respondents:

- Support Federated IdM for Cruise Planning, Captive Portal, Science Logging, and File Sharing
- Are mixed or do not support Federated IdM for Email, Kiosks, VDI, SysAdmin, Ops Tech, Vessel Maintenance
- Agree that Federated IdM should never block logins if the Internet is down
  Strongly desire the ability to administer identities from vessel networks
- Agree that federated IdM will be opt-in on a per vessel per service basis

Milestone 2: Recommended Solution



InCommon

43 of 58 UNOLS Institutions are in the InCommon Federation

GMail

Google Apps for Education and other GMail Accounts

CILogon

ARF IdM Services

Shoreside Fleetwide AuthN + AuthZ Services

COmanage

Grouper

OpenLDAP

FreeIPA

Active Directory

OpenID 2

ARF Shoreside Services

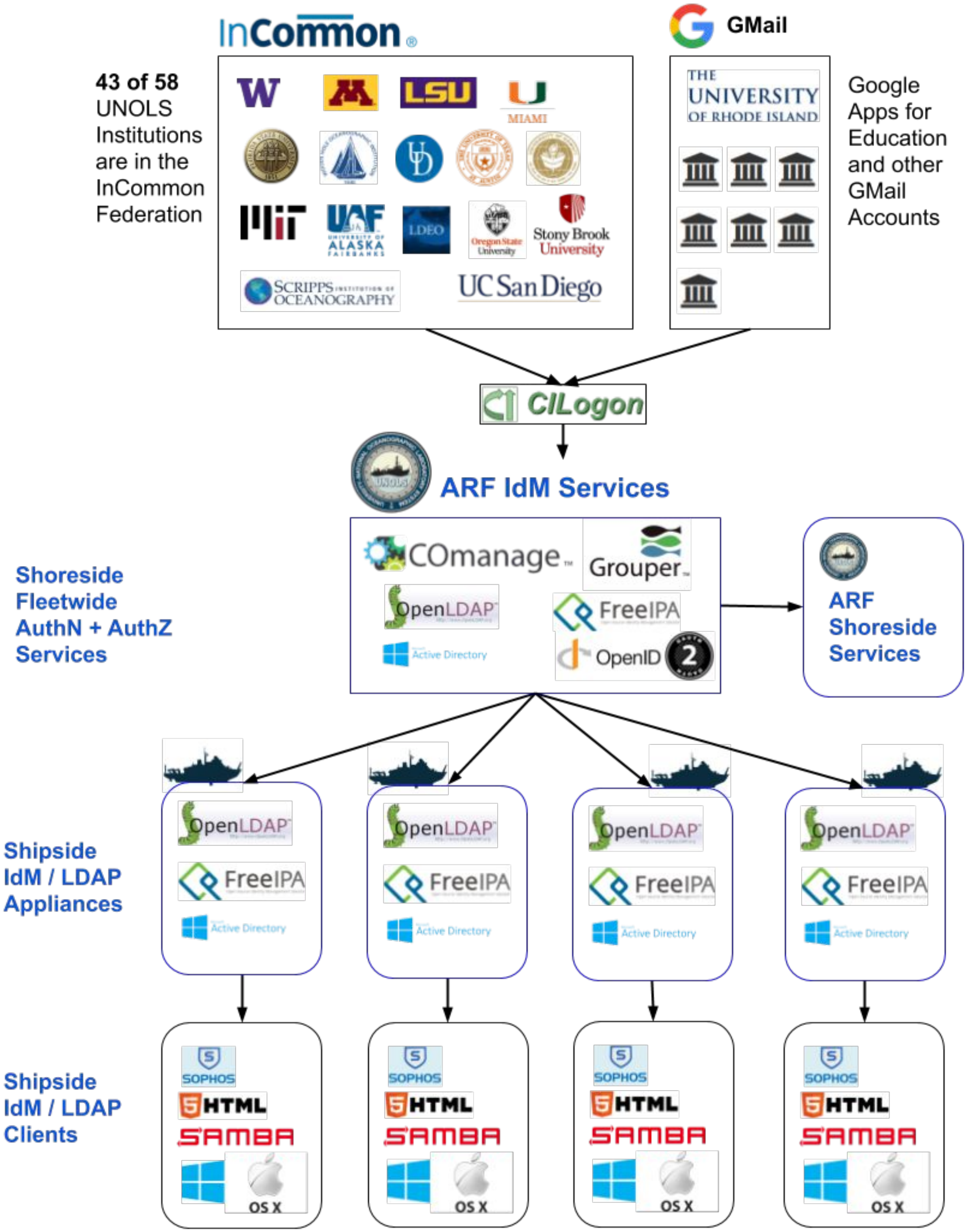
Shipside IdM / LDAP Appliances

Shipside IdM / LDAP Clients

W
LSU
MIAMI
MIT
UAF UNIVERSITY OF ALASKA FAIRBANKS
LDEO
Oregon State University
Stony Brook University
SCRIPPS INSTITUTION OF OCEANOGRAPHY
UC San Diego
THE UNIVERSITY OF RHODE ISLAND
SOPHOS
HTML
SAMBA
OS X

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI COE pilot



InCommon

GMail

43 of 58 UNOLS Institutions are in the InCommon Federation

Google Apps for Education and other GMail Accounts

CILogon

ARF IdM Services

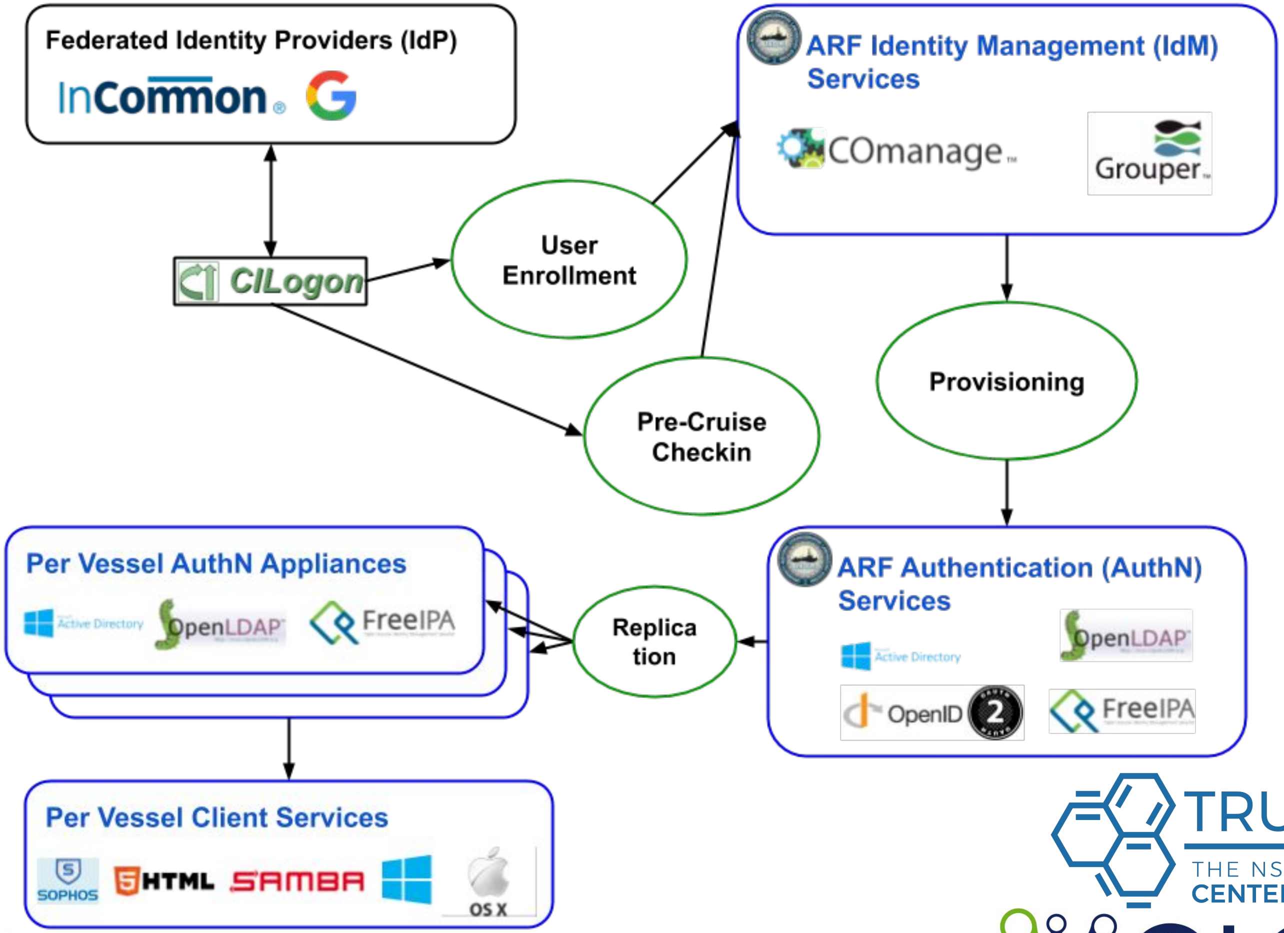
Shoreside Fleetwide AuthN + AuthZ Services

ARF Shoreside Services

Shipside IdM / LDAP Appliances

Shipside IdM / LDAP Clients

IdM Workflow



TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

R/V Sikuliaq

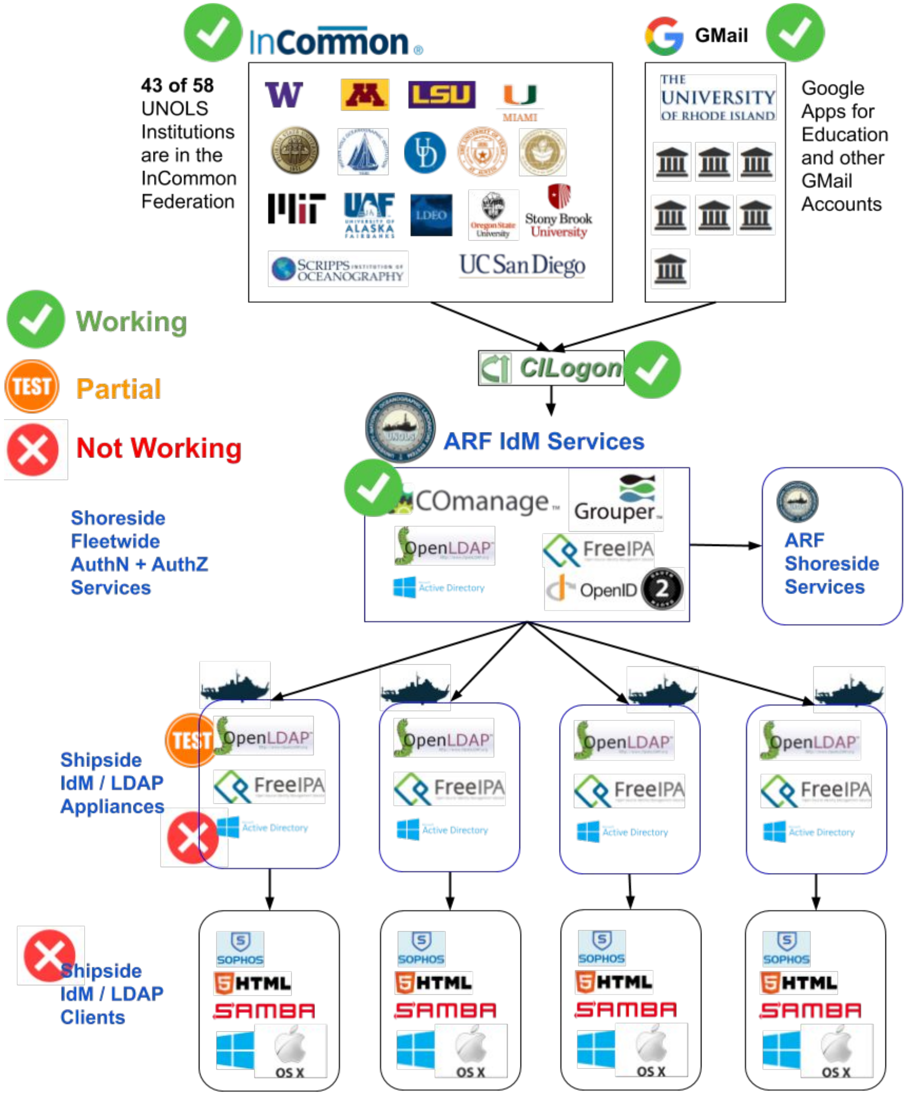
College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

Milestone 3:
Proof of Concept

How far did we get?

- Working InCommon / Google Federation
- Working ARF COManage Instance
- Partial Open LDAP Server
- Incomplete AD Server
- Incomplete Samba Client



✓ Working

TEST Partial

✗ Not Working

✓ InCommon

43 of 58 UNOLS Institutions are in the InCommon Federation

✓ GMail

Google Apps for Education and other GMail Accounts

✓ CILogon

ARF IdM Services

✓ COmanage, Grouper, OpenLDAP, FreeIPA, Active Directory, OpenID 2

Shoreside Fleetwide AuthN + AuthZ Services

ARF Shoreside Services

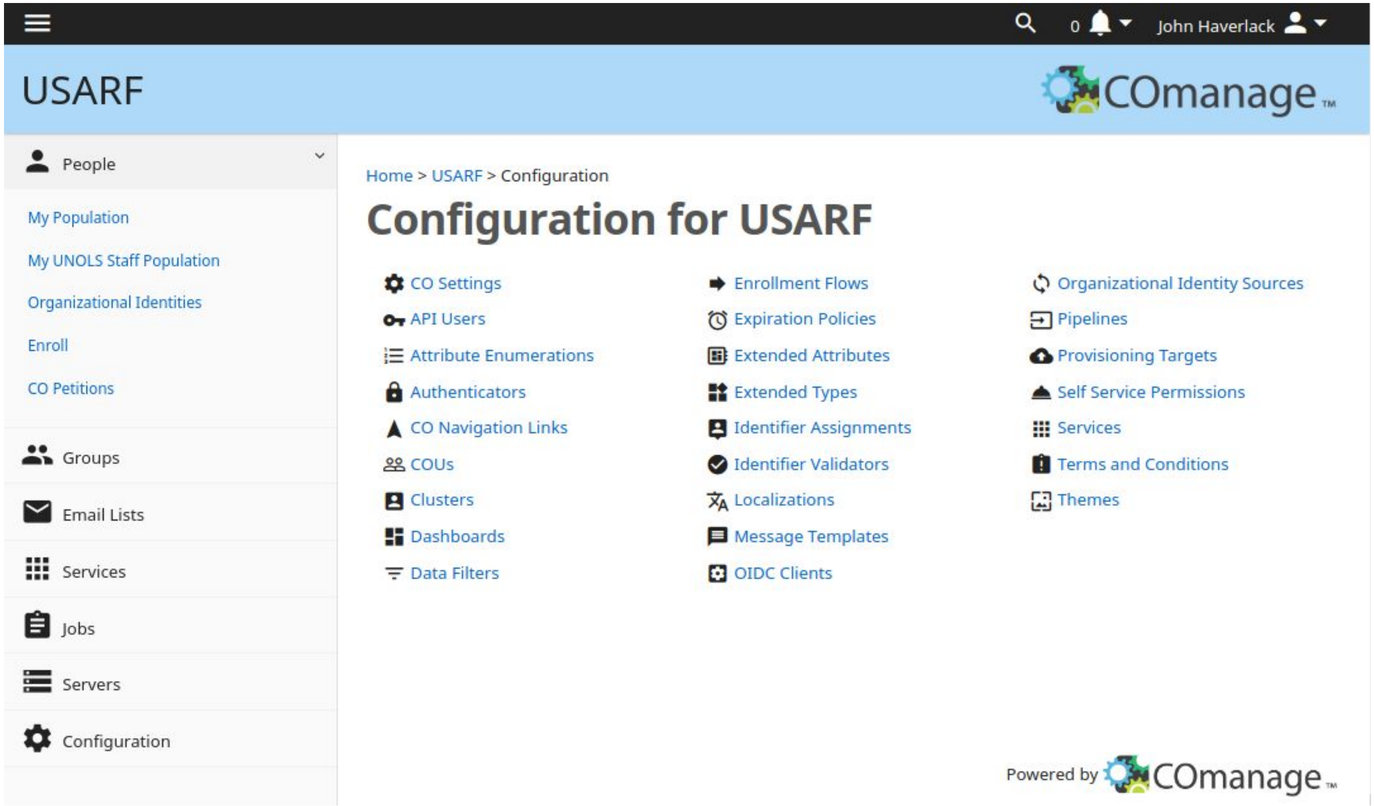
Shipside IdM / LDAP Appliances

Shipside IdM / LDAP Clients

COmanage™ CILogon

Federated Authentication

COmanage™



John Haverlack

USARF

People

- My Population
- My UNOLS Staff Population
- Organizational Identities
- Enroll
- CO Petitions

Groups

Email Lists

Services

Jobs

Servers

Configuration

Home > USARF > Configuration

Configuration for USARF

- CO Settings
- API Users
- Attribute Enumerations
- Authenticators
- CO Navigation Links
- COUs
- Clusters
- Dashboards
- Data Filters
- Enrollment Flows
- Expiration Policies
- Extended Attributes
- Extended Types
- Identifier Assignments
- Identifier Validators
- Localizations
- Message Templates
- OIDC Clients
- Organizational Identity Sources
- Pipelines
- Provisioning Targets
- Self Service Permissions
- Services
- Terms and Conditions
- Themes

Powered by COmanage™

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

CI CoE PILOT

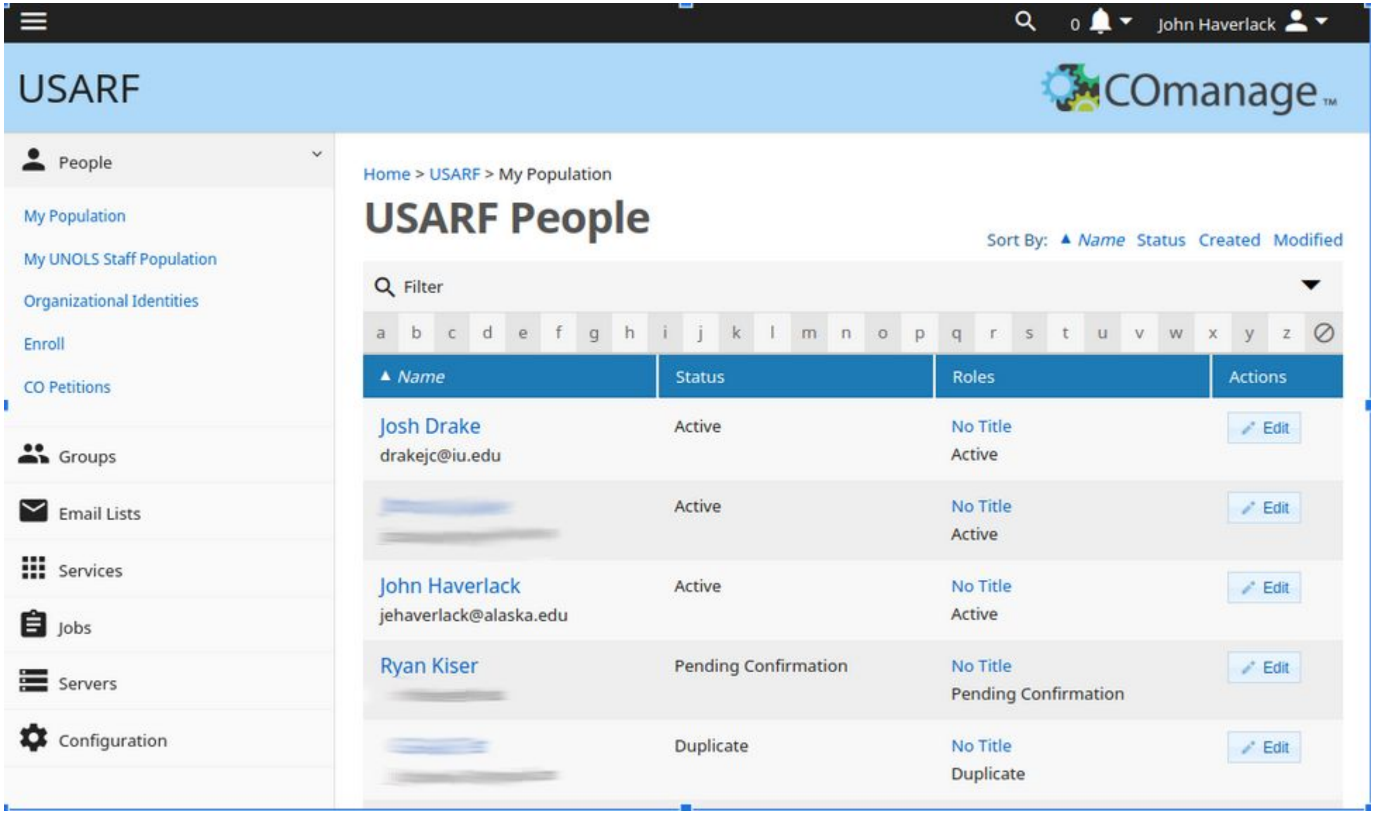
UAF UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

COmanage™



Home > USARF > My Population

USARF People

Sort By: ▲ *Name* Status Created Modified

Filter

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 ⊘

▲ *Name*	Status	Roles	Actions
Josh Drake drakejc@iu.edu	Active	No Title Active	Edit
[redacted]	Active	No Title Active	Edit
John Haverlack jehaverlack@alaska.edu	Active	No Title Active	Edit
Ryan Kiser [redacted]	Pending Confirmation	No Title Pending Confirmation	Edit
[redacted]	Duplicate	No Title Duplicate	Edit

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

UNIVERSITY OF ALASKA FAIRBANKS

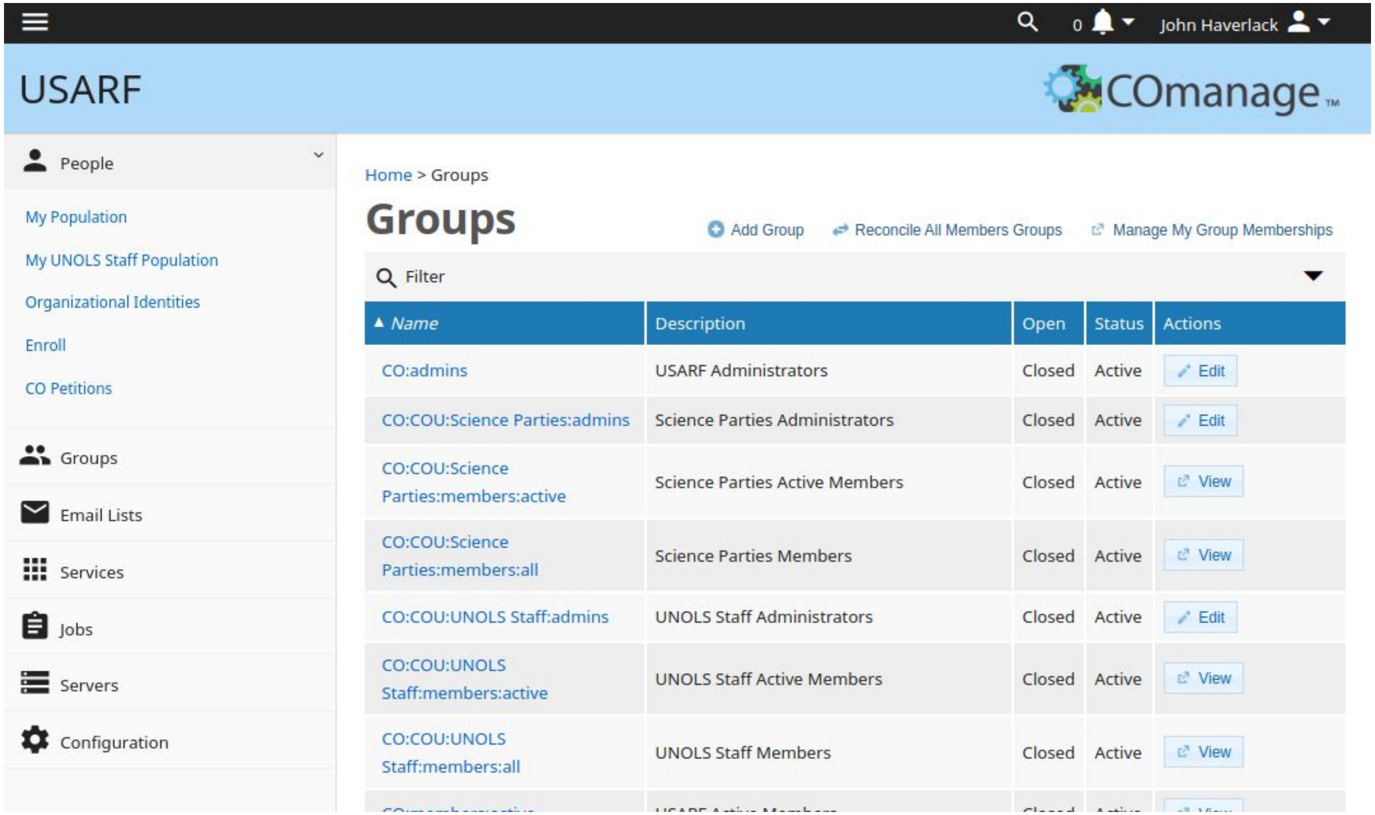
R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

CFOS UNOLS NSF

COmanage™



- People
  - My Population
  - My UNOLS Staff Population
  - Organizational Identities
  - Enroll
  - CO Petitions
- Groups
- Email Lists
- Services
- Jobs
- Servers
- Configuration

Home > Groups

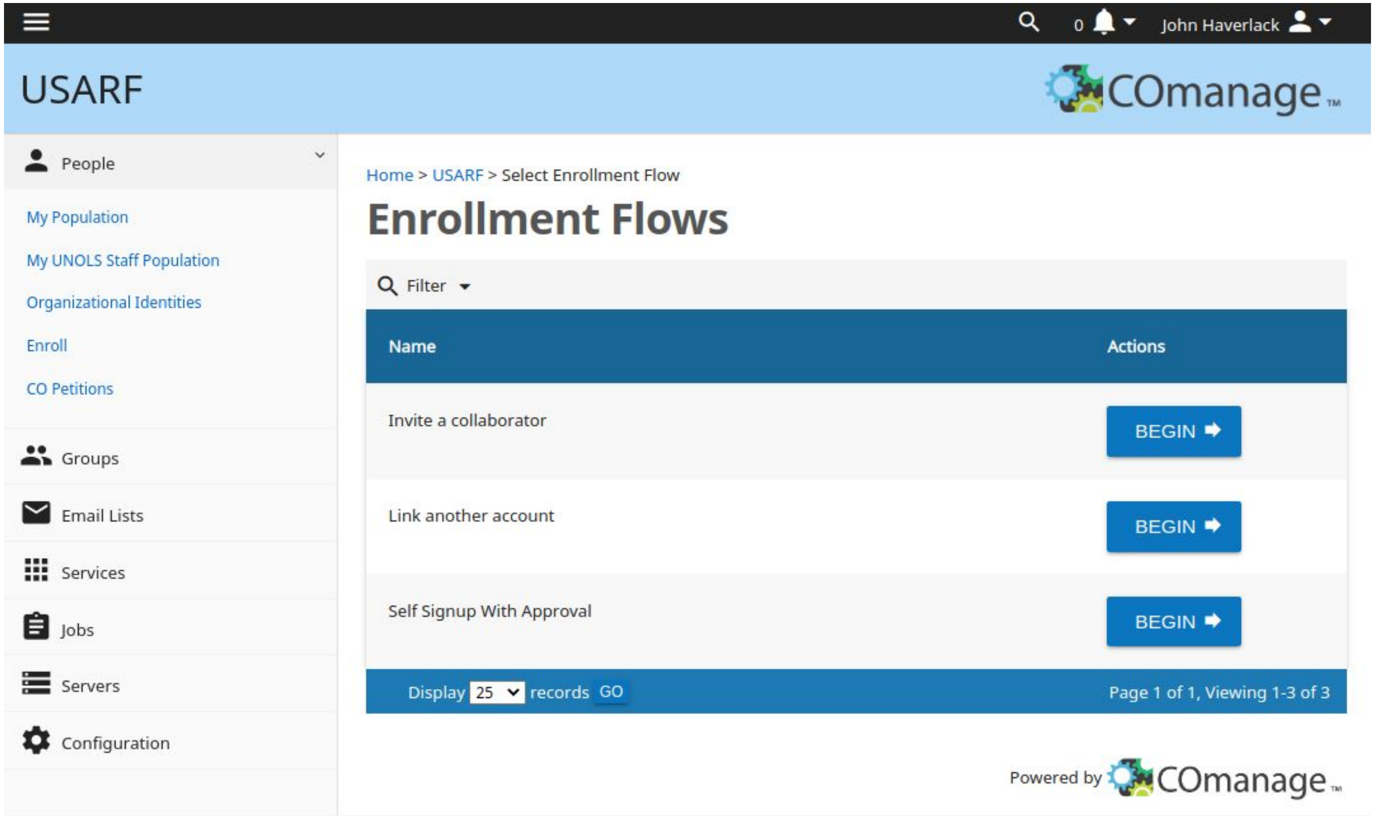
Groups

Add Group · Reconcile All Members Groups · Manage My Group Memberships

Filter

▲ Name	Description	Open	Status	Actions
CO:admins	USARF Administrators	Closed	Active	Edit
CO:COU:Science Parties:admins	Science Parties Administrators	Closed	Active	Edit
CO:COU:Science Parties:members:active	Science Parties Active Members	Closed	Active	View
CO:COU:Science Parties:members:all	Science Parties Members	Closed	Active	View
CO:COU:UNOLS Staff:admins	UNOLS Staff Administrators	Closed	Active	Edit
CO:COU:UNOLS Staff:members:active	UNOLS Staff Active Members	Closed	Active	View
CO:COU:UNOLS Staff:members:all	UNOLS Staff Members	Closed	Active	View
CO:members:active	USARF Active Members	Closed	Active	View

COmanage™



Home > USARF > Select Enrollment Flow

Enrollment Flows

Name	Actions
Invite a collaborator	BEGIN ➡
Link another account	BEGIN ➡
Self Signup With Approval	BEGIN ➡

Display 25 records GO   Page 1 of 1, Viewing 1-3 of 3

Powered by COmanage

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

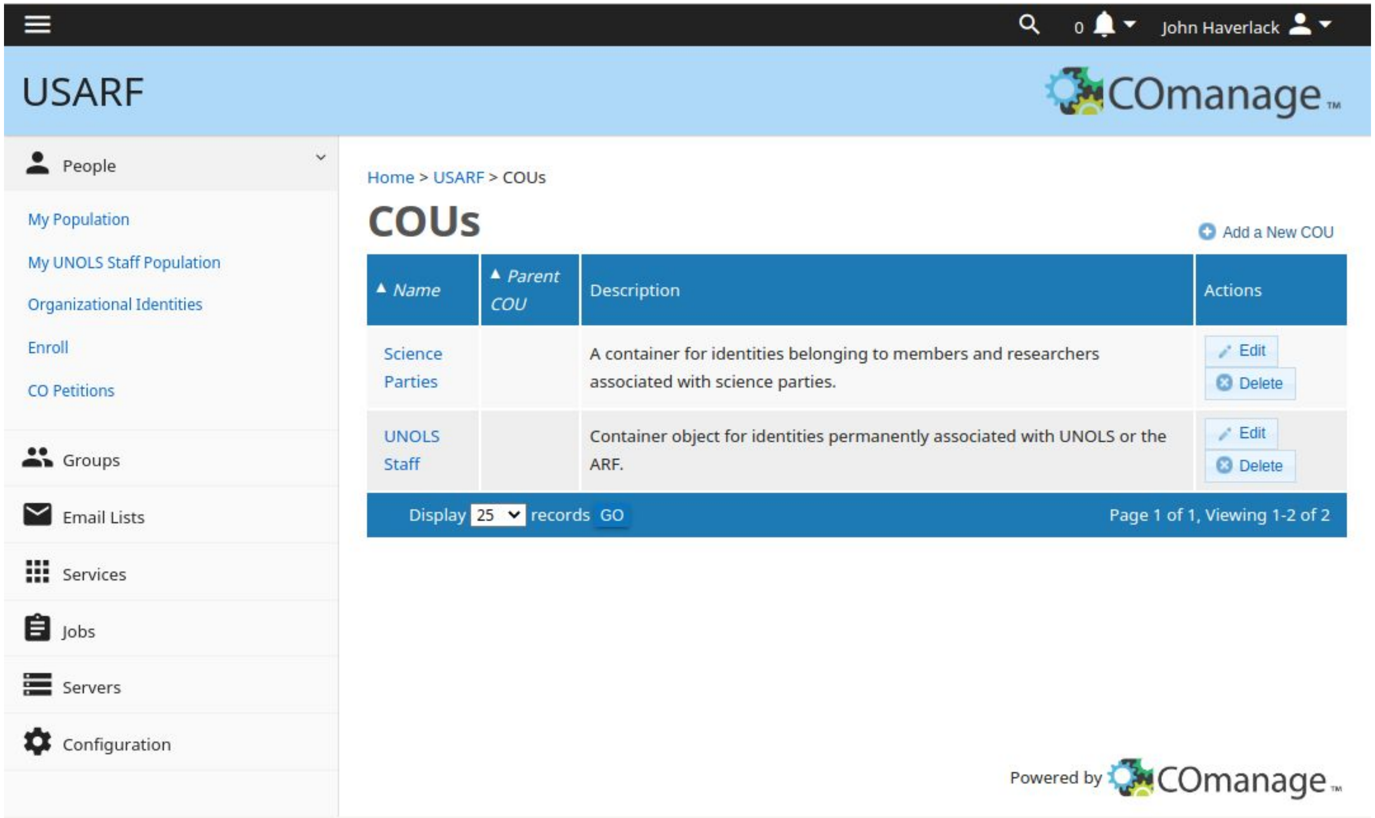
CI CoE PILOT

R/V Sikuliaq

College of Fisheries and Ocean Sciences

https://www.sikuliaq.alaska.edu

COmanage™



Home > USARF > COUs

COUs

▲ *Name*	▲ *Parent COU*	Description	Actions
Science Parties		A container for identities belonging to members and researchers associated with science parties.	Edit Delete
UNOLS Staff		Container object for identities permanently associated with UNOLS or the ARF.	Edit Delete

Display 25 records GO — Page 1 of 1, Viewing 1-2 of 2

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

UNIVERSITY OF ALASKA FAIRBANKS

R/V Sikuliaq

College of Fisheries and Ocean Sciences

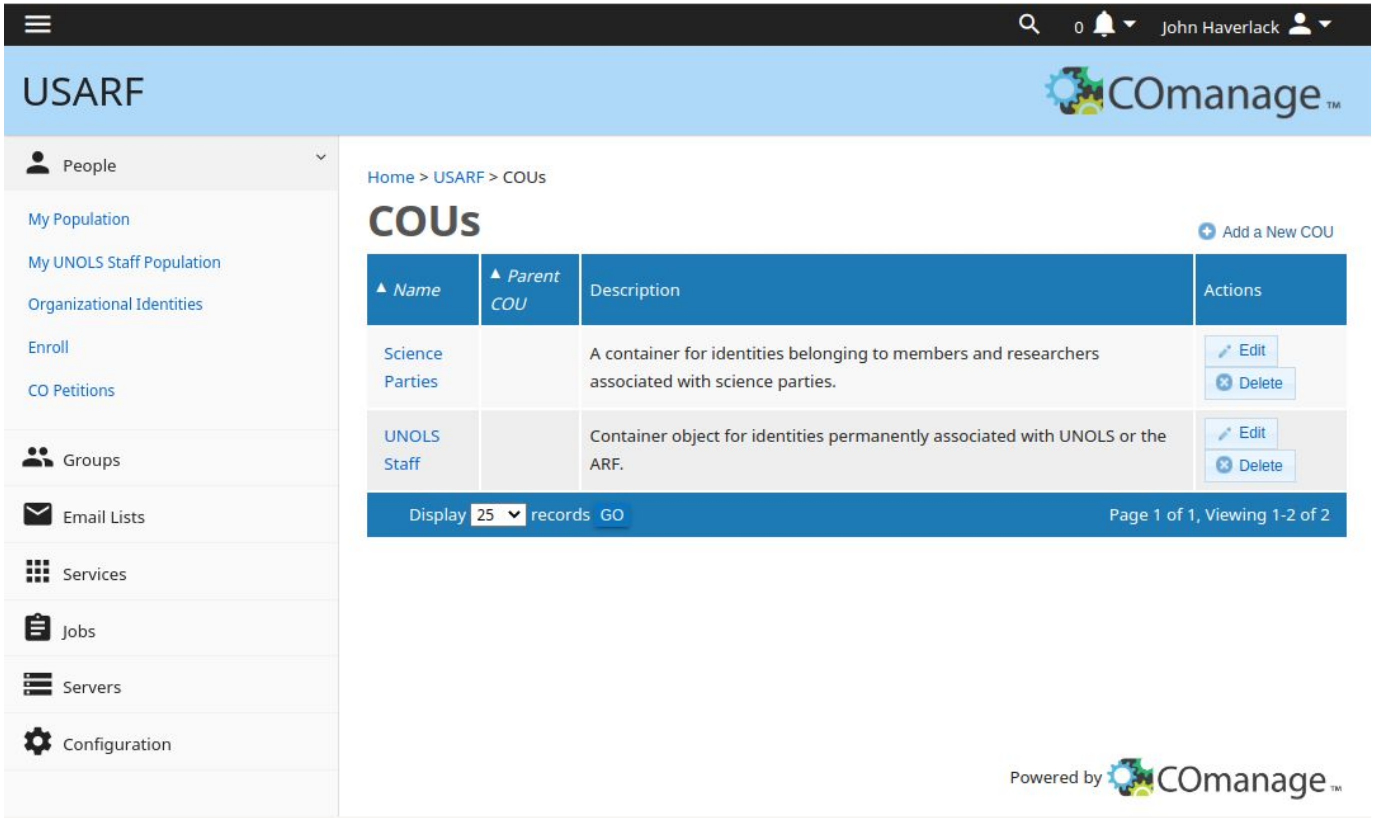
https://www.sikuliaq.alaska.edu

CFOS

UNOLS

NSF

COmanage™



Home > USARF > COUs

COUs

Add a New COU

▲ *Name*	▲ *Parent COU*	Description	Actions
Science Parties		A container for identities belonging to members and researchers associated with science parties.	Edit Delete
UNOLS Staff		Container object for identities permanently associated with UNOLS or the ARF.	Edit Delete

Display 25 records GO — Page 1 of 1, Viewing 1-2 of 2

Challenges

- Identity Management is Complicated
- There is more than one way to organize identity data
- Integrating authentication systems is hard
- Bi-directional administration (ship to shore) is not currently available
- CILogon annual subscription: ~$9,000 per year

There are resources that can help us.

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

CI CoE PILOT

Next Steps

- Write a **Federated Identity Management Service** Proposal
    - Available to U.S. ARF on a **per vessel / per service Opt-In** basis
    - Would pursue potential collaborations with
        - CILogon
        - CICoE
        - Trusted CI
        - Marine Facilities Planner (IdM Client)
    - Request funding to establish and run IdM service for 5 years

TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

CI CoE PILOT