

# 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



**R/V Sikuliaq**

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



# ARF IdM Engagement Plan

[https://docs.google.com/document/d/1Btb4VRaXrZzg\\_8brZ\\_viSMY20PNH-AlcTnamwvr22Ss/edit](https://docs.google.com/document/d/1Btb4VRaXrZzg_8brZ_viSMY20PNH-AlcTnamwvr22Ss/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



**R/V Sikuliaq**  
College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



# 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



*R/V Sikuliaq*

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



# IdM Primer Video

## IdM Primer Video

<https://youtu.be/rZWOXeOsN6E>

## IdM Primer Presentation

[https://docs.google.com/presentation/d/1\\_riLUbkQYiqvOsPXezn3GLwehj1WEWLwfiELo4qwxIE/edit?usp=sharing](https://docs.google.com/presentation/d/1_riLUbkQYiqvOsPXezn3GLwehj1WEWLwfiELo4qwxIE/edit?usp=sharing)

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



*R/V Sikuliaq*

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



# 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



*R/V Sikuliaq*

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



# 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



*R/V Sikuliaq*

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



# Milestone 2: Recommended Solution

43 of 58  
UNOLS  
Institutions  
are in the  
InCommon  
Federation

InCommon



GMail



Google  
Apps for  
Education  
and other  
GMail  
Accounts

CI Logon



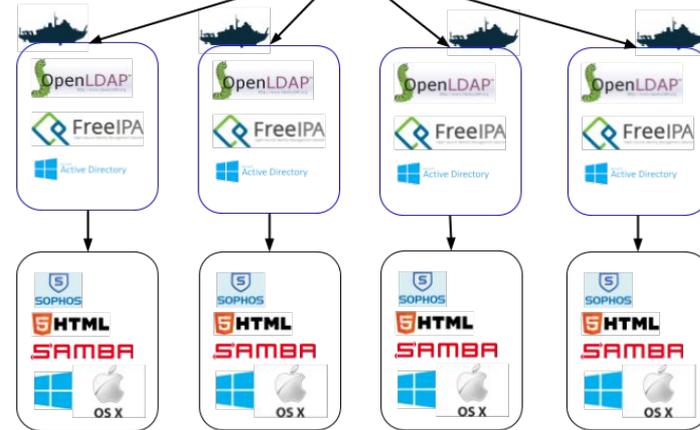
ARF IdM Services

Shoreside  
Fleetwide  
AuthN + AuthZ  
Services



ARF  
Shoreside  
Services

Shipside  
IdM / LDAP  
Appliances



Shipside  
IdM / LDAP  
Clients



*R/V Sikuliaq*

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



InCommon®

GMail

43 of 58 UNOLS Institutions are in the InCommon Federation



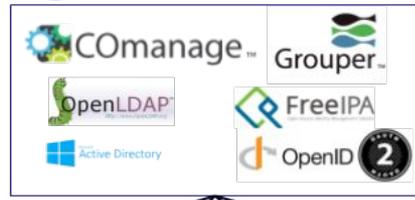
Google Apps for Education and other Gmail Accounts

CI Logon



ARF IdM Services

Shoreside Fleetwide AuthN + AuthZ Services



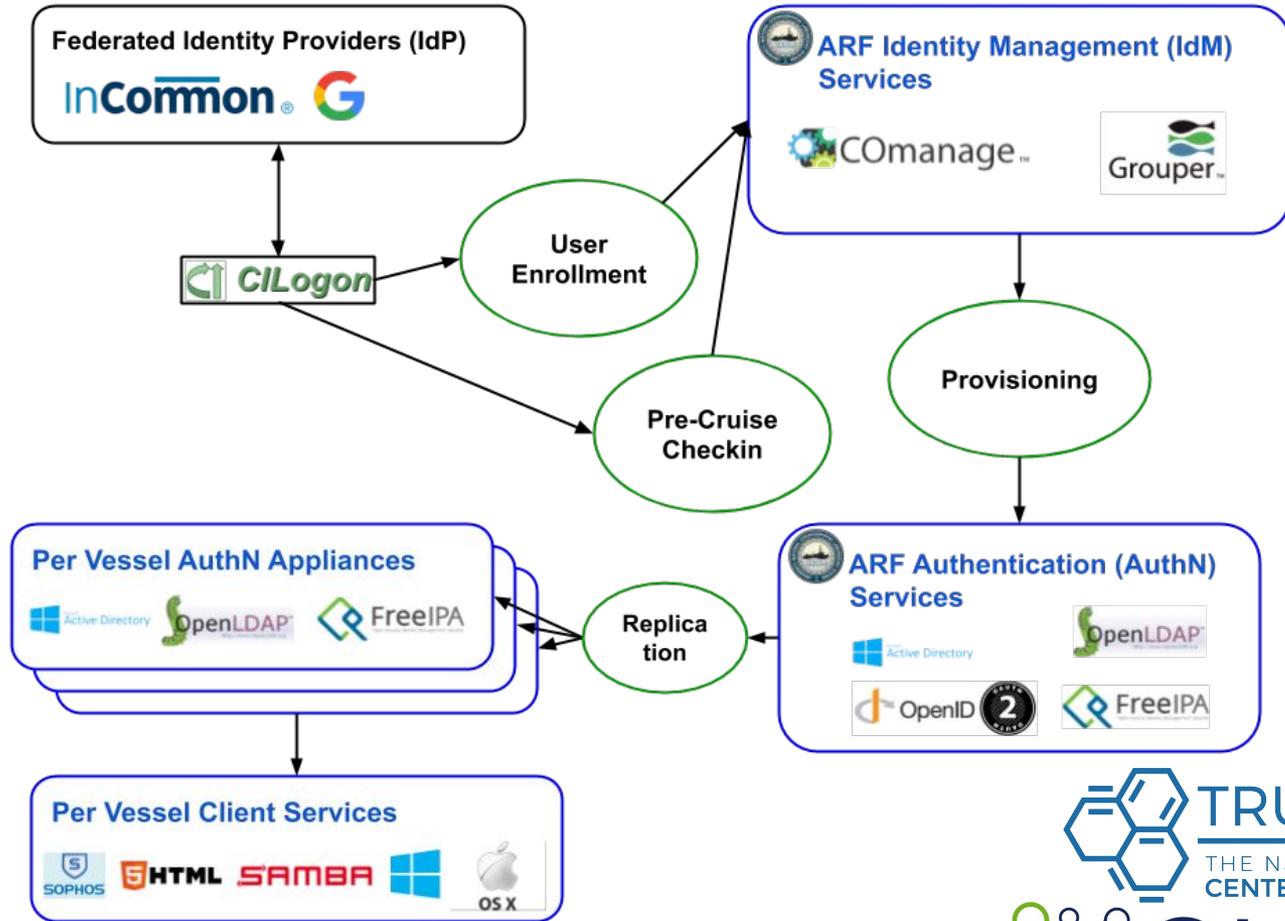
Shipside IdM / LDAP Appliances



Shipside IdM / LDAP Clients



# IdM Workflow



**R/V Sikuliaq**  
College of Fisheries and Ocean Sciences

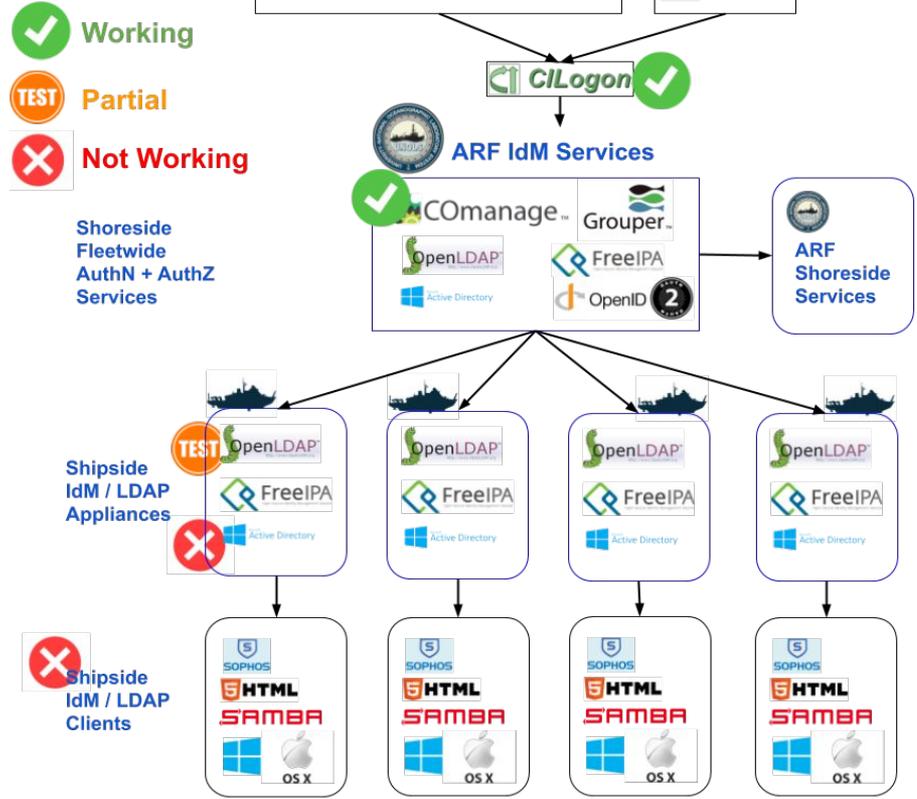
<https://www.sikuliaq.alaska.edu>



# Milestone 3: Proof of Concept

How far did we get?

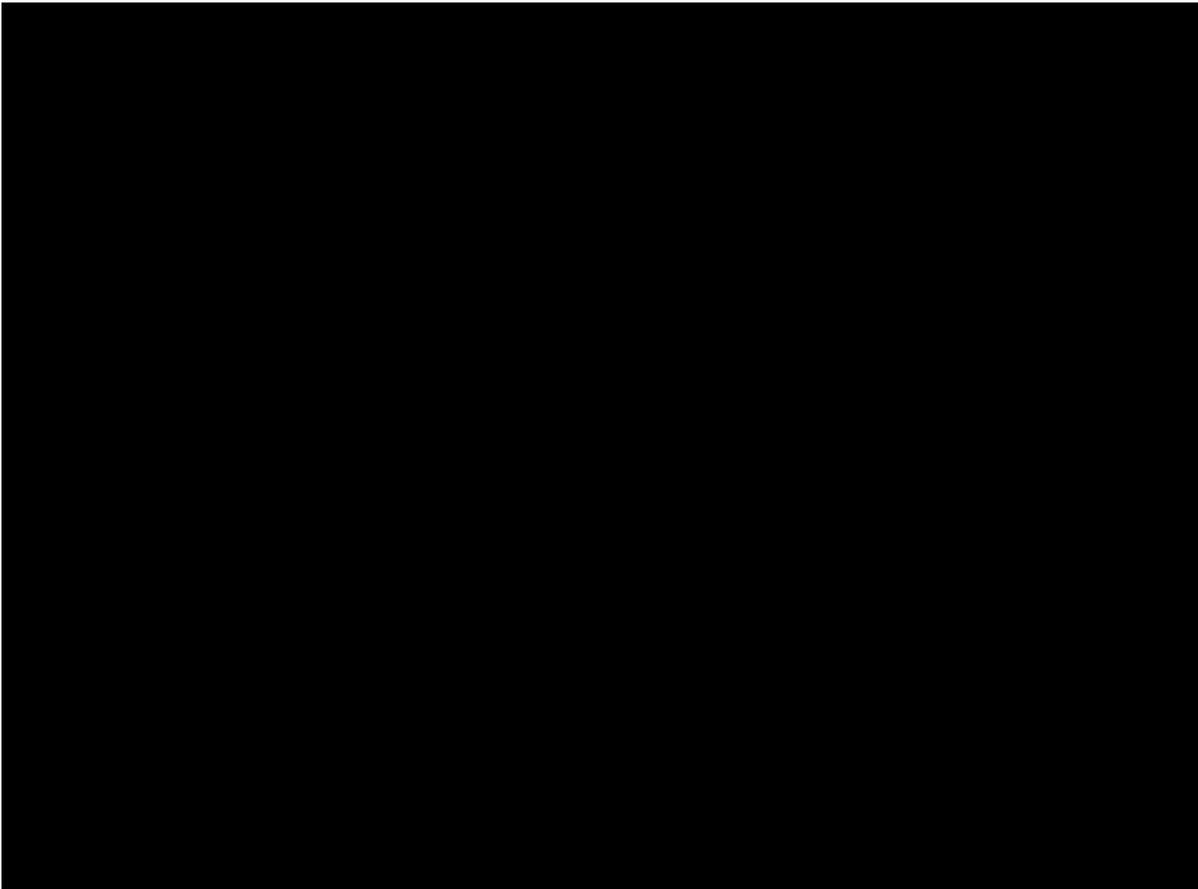
- Working InCommon / Google Federation
- Working ARF COManage Instance
- Partial Open LDAP Server
- Incomplete AD Server
- Incomplete Samba Client



**R/V Sikuliaq**  
College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>





# Federated Authentication

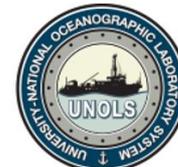
<https://drive.google.com/file/d/1-fXr5xxzAQ6m55ng5FYc6R0UKfgTwHsS/view?usp=sharing>



*R/V Sikuliaq*

College of Fisheries and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



☰
🔍 0 🔔 John Haverlack 👤

USARF


**COmanage™**

**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

<ul style="list-style-type: none"> <li>⚙️ CO Settings</li> <li>🔑 API Users</li> <li>☰ Attribute Enumerations</li> <li>🔒 Authenticators</li> <li>📍 CO Navigation Links</li> <li>👤 COUs</li> <li>📁 Clusters</li> <li>📊 Dashboards</li> <li>🗑️ Data Filters</li> </ul>	<ul style="list-style-type: none"> <li>➔ Enrollment Flows</li> <li>🕒 Expiration Policies</li> <li>📄 Extended Attributes</li> <li>📁 Extended Types</li> <li>👤 Identifier Assignments</li> <li>✅ Identifier Validators</li> <li>🌐 Localizations</li> <li>📄 Message Templates</li> <li>🔌 OIDC Clients</li> </ul>	<ul style="list-style-type: none"> <li>🔄 Organizational Identity Sources</li> <li>📡 Pipelines</li> <li>🎯 Provisioning Targets</li> <li>⚡ Self Service Permissions</li> <li>☰ Services</li> <li>📄 Terms and Conditions</li> <li>🖨️ Themes</li> </ul>
---	---	---

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>



 0  John Haverlack 

USARF



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

Home > USARF > My Population

## USARF People

Sort By: ▲ Name Status Created Modified

Q 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	<a href="#">Edit</a>
██████████	Active	No Title Active	<a href="#">Edit</a>
John Haverlack jehaverlack@alaska.edu	Active	No Title Active	<a href="#">Edit</a>
Ryan Kiser	Pending Confirmation	No Title Pending Confirmation	<a href="#">Edit</a>
██████████	Duplicate	No Title Duplicate	<a href="#">Edit</a>



R/V Sikuliaq

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



- 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	<a href="#">Edit</a>
CO:COU:Science Parties:admins	Science Parties Administrators	Closed	Active	<a href="#">Edit</a>
CO:COU:Science Parties:members:active	Science Parties Active Members	Closed	Active	<a href="#">View</a>
CO:COU:Science Parties:members:all	Science Parties Members	Closed	Active	<a href="#">View</a>
CO:COU:UNOLS Staff:admins	UNOLS Staff Administrators	Closed	Active	<a href="#">Edit</a>
CO:COU:UNOLS Staff:members:active	UNOLS Staff Active Members	Closed	Active	<a href="#">View</a>
CO:COU:UNOLS Staff:members:all	UNOLS Staff Members	Closed	Active	<a href="#">View</a>



**R/V Sikuliaq**  
College of Fisheries and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



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

Home > USARF > Select Enrollment Flow

## Enrollment Flows

Filter

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™



**R/V Sikuliaq**

College of Fisheries and Ocean Sciences

<https://www.sikuliaq.alaska.edu>



- 👤 People
- My Population
- My UNOLS Staff Population
- Organizational Identities
- Enroll
- CO Petitions
- 👥 Groups
- ✉️ Email Lists
- 🗄️ Services
- 📅 Jobs
- 🖨️ Servers
- ⚙️ Configuration

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.	<a href="#">Edit</a> <a href="#">Delete</a>
UNOLS Staff		Container object for identities permanently associated with UNOLS or the ARF.	<a href="#">Edit</a> <a href="#">Delete</a>

Display **25** records [GO](#) Page 1 of 1, Viewing 1-2 of 2

Powered by  COmanage™



**R/V Sikuliaq**  
**College of Fisheries and Ocean Sciences**

<https://www.sikuliaq.alaska.edu>



- 👤 People
- My Population
- My UNOLS Staff Population
- Organizational Identities
- Enroll
- CO Petitions
- 👥 Groups
- ✉️ Email Lists
- 🏠 Services
- 📅 Jobs
- 🖨️ Servers
- ⚙️ Configuration

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.	<a href="#">Edit</a> <a href="#">Delete</a>
UNOLS Staff		Container object for identities permanently associated with UNOLS or the ARF.	<a href="#">Edit</a> <a href="#">Delete</a>

Display **25** records [GO](#) Page 1 of 1, Viewing 1-2 of 2

Powered by  COmanage™



**R/V Sikuliaq**  
**College of Fisheries and Ocean Sciences**

<https://www.sikuliaq.alaska.edu>



# 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.**



***R/V Sikuliaq***

**College of Fisheries  
and Ocean Sciences**

<https://www.sikuliaq.alaska.edu>



# 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
    - CCoE
    - Trusted CI
    - Marine Facilities Planner (IdM Client)
  - Request funding to establish and run IdM service for 5 years



*R/V Sikuliaq*

College of Fisheries  
and Ocean Sciences

<https://www.sikuliaq.alaska.edu>

