InCommon.org

Change is Afoot: Navigating Cloud Shifts in Higher Ed IAM

IAM Online – March 2025

Speakers:

Tommy Doan - Identity Management Lead | Southern Methodist University
Kellen Murphy - Identity Architect | University of Virginia

Moderator:

Grady Bailey - Senior IAM Architect | Internet2

AGENDA

1. Welcome
2. Introductions
3. Presentation
4. Q&A
5. Closing

Welcome

REMINDERS

- We’re taking questions and comments live using the **Zoom Q&A function**, so please send those messages during the presentation because we want this to be as interactive as possible.

- Also feel free to post messages **in the chat**. Just be sure when you are posting, your message is being sent to everyone, from the drop-down menu options.

- We are also recording this webinar, you will receive the link to the recording via email, and it will be posted on the **InCommon website** and on our **IAM Online YouTube channel** soon!

Introductions

Today's Speakers

Kellen Murphy
Identity Architect

University of Virginia

Tommy Doan
Identity Management Lead

Southern Methodist University

Grady Bailey
Senior IAM Architect

Internet2

MODERATOR

Presentation

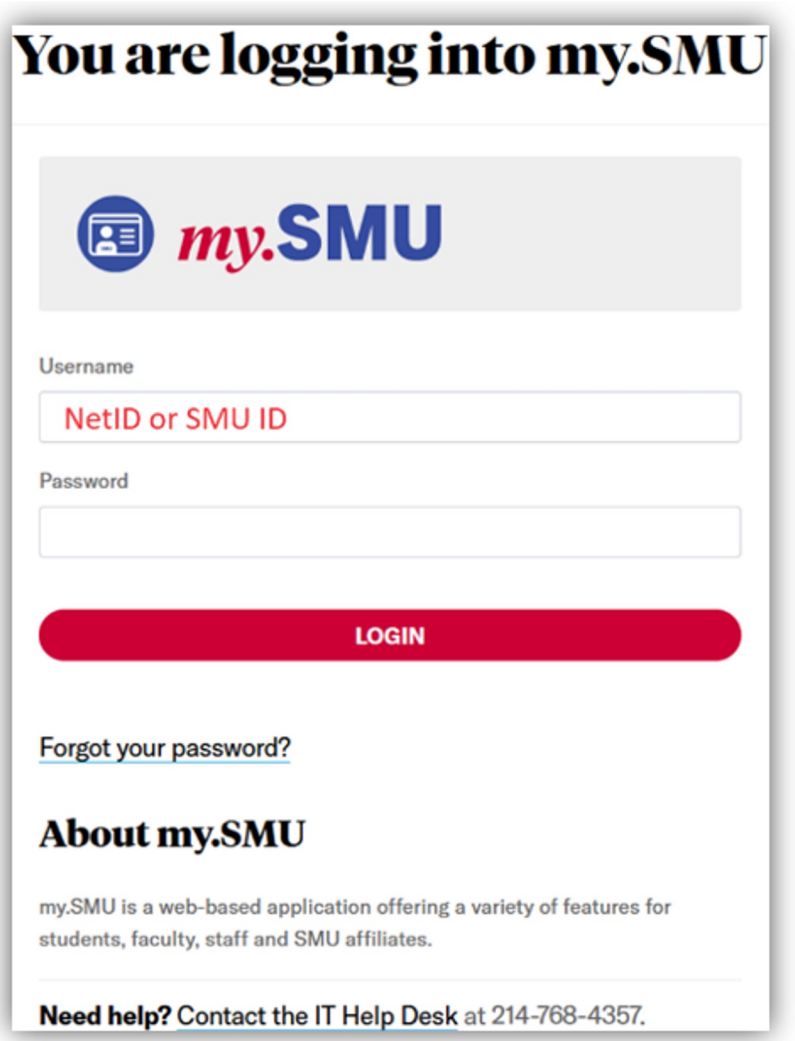
Southern Methodist University

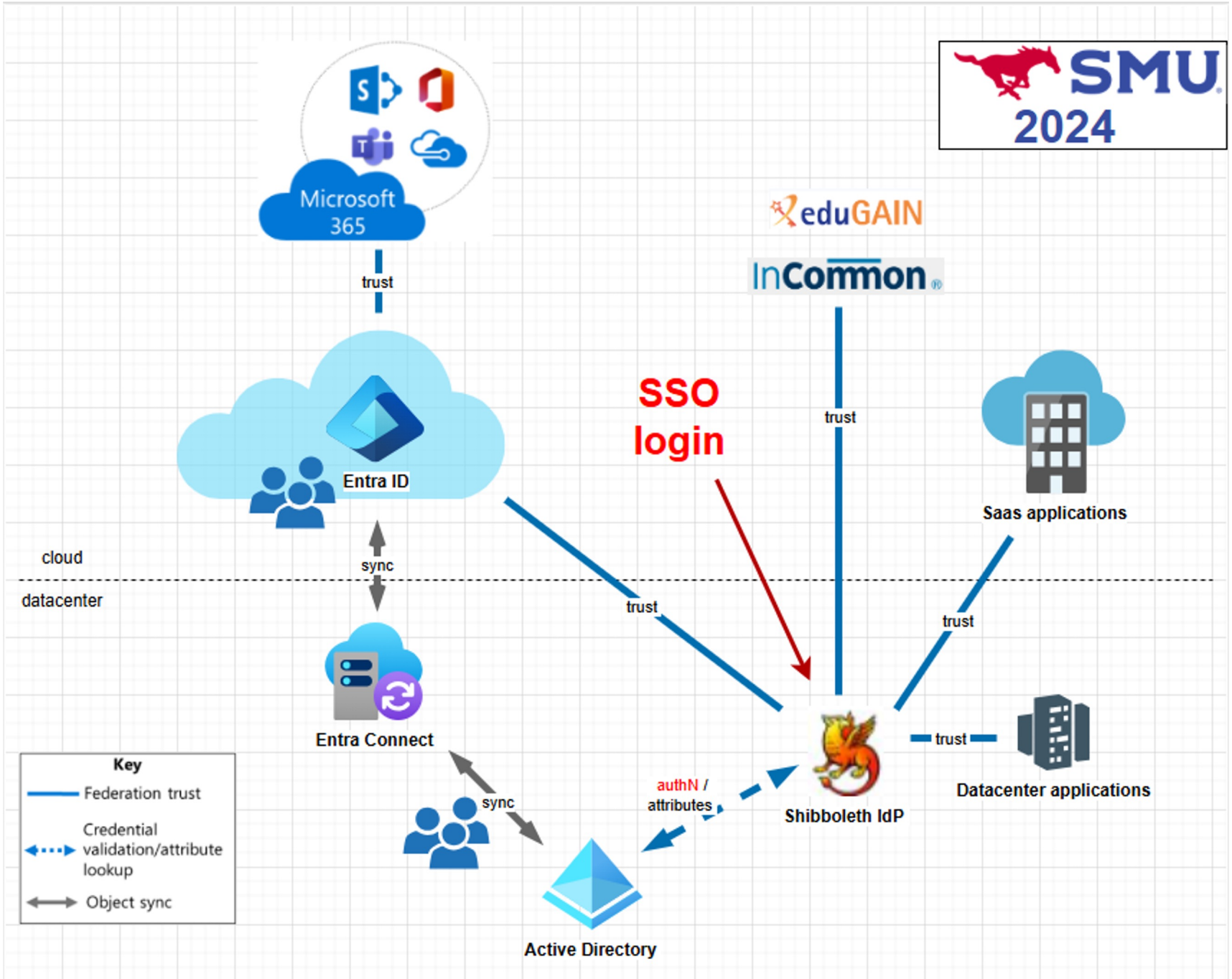
Identity and Access Management

World Changers Shaped Here SMU

- 3 IAM team members
- 12,000 students
- 3,500 employees
- 85,000 user accounts

SMU's SSO logon page in 2024 (prior to our changes)




SMU
2024
Microsoft 365
trust
eduGAIN
InCommon
SSO login
trust
Saas applications
Entra ID
cloud
sync
datacenter
trust
trust
Entra Connect
trust
Datacenter applications
Key
Federation trust
Credential validation/attribute lookup
Object sync
sync
authN / attributes
Shibboleth IdP
Active Directory

2024 architecture description

Active Directory		
	single domain	yes
	enterprise directory service	yes
SSO service		
		Shibboleth IdP
Entra ID		
	Entra Connect for sync	yes
	authentication source	Shibboleth IdP
Shibboleth IdP		
	authentication source	Active Directory (direct)
	attribute resolver	Active Directory
	local SAML SPs	~100
	total SAML SPs	~300
Duo integration		
		Shibboleth IdP

Motivations for change

- **Windows Hello for Business**
  - A collection of Microsoft's password-less solutions.
- **Microsoft Intune**
  - Microsoft's endpoint management for the cloud.

- Both require a Primary Refresh Token (PRT) to be issued during SSO logons.

- General direction toward the Microsoft cloud.

- Gradual transition away from Active Directory.

Project management details

- Initial discussions began in July 2023.
- The project kicked off in Spring 2024.
- Implementation occurred just after midnight Thursday December 26, 2024.
  - This difficult decision was based on several factors:
    - Plan for things to not go as planned.
    - Contingency dates were available.
    - Minimize user impact.
    - IT help desk staffing during the holiday season.

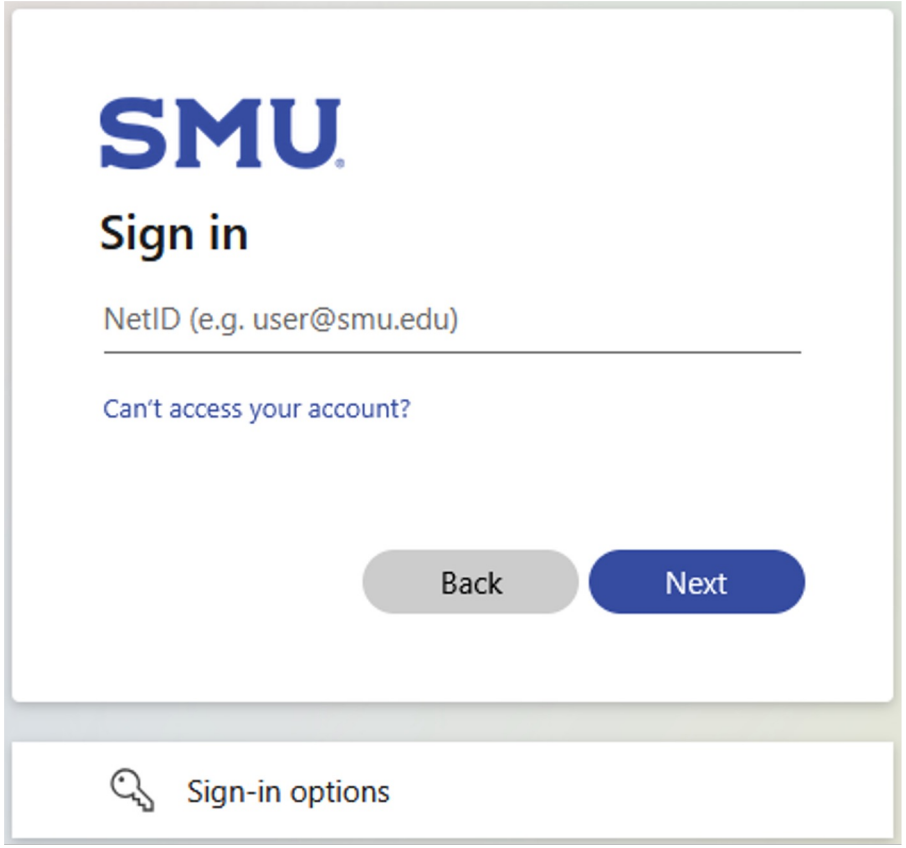
Prepare our users

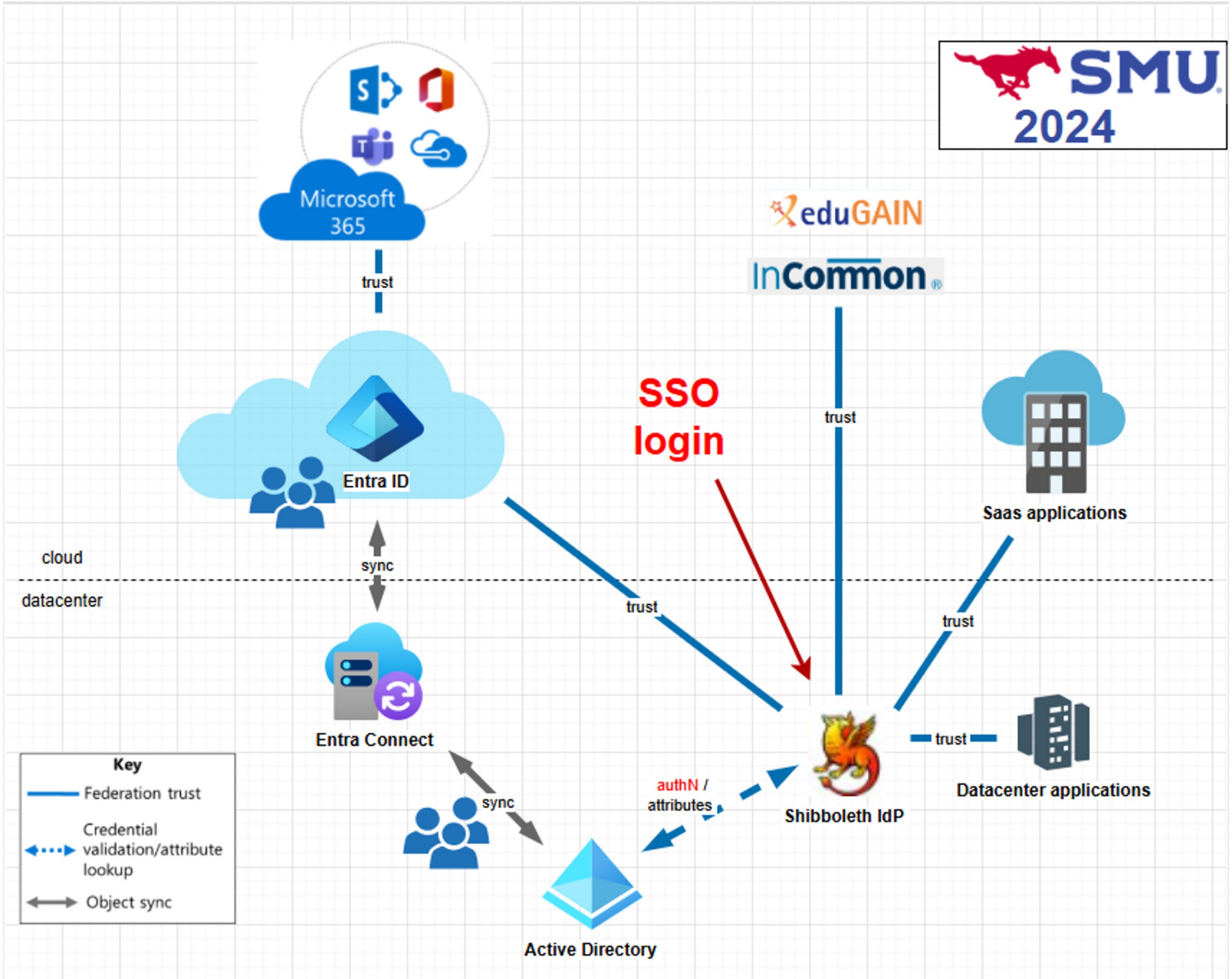
- Introduce the NetID
  - **userPrincipalName** (UPN) required for Entra ID logons.
  - Our users login with their **sAMAccountName**, known as the “SMU ID.”
  - These are two very different values in our environment.
  - We configured our Shibboleth IdP to support both values for user logon.
  - Gathered metrics on adoption of the NetID.

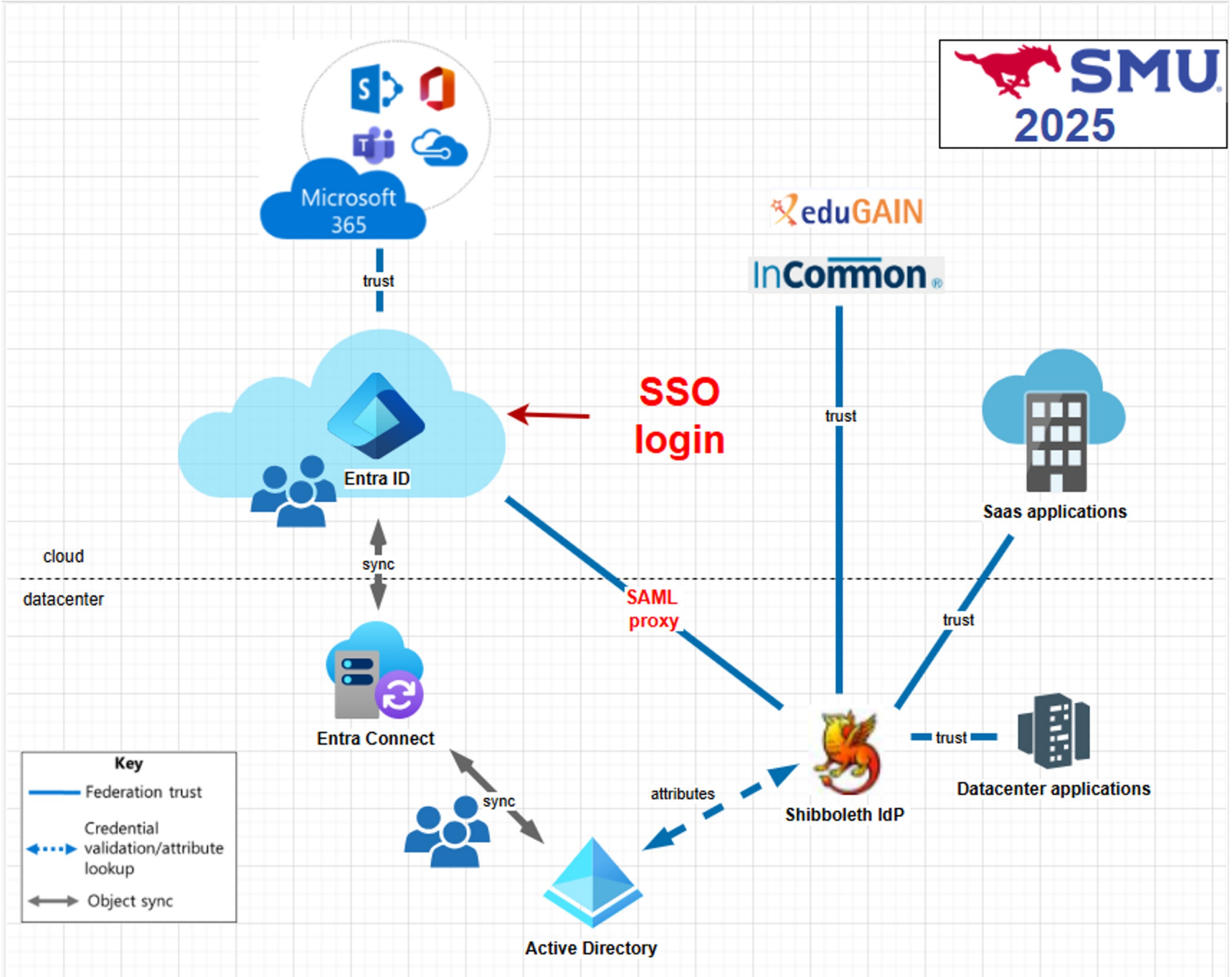
- Develop the MyProfile page
  - Lookup profile information, including the NetID.
  - We gathered metrics on visits to the MyProfile page.

- Start a massive communication campaign in October
  - Include the MyProfile page and the NetID.
  - New SSO logon page.
  - More than 100,000 email messages, digital displays, social media, etc.

SMU's SSO logon page in 2025 (after our changes)




SMU
2024
Microsoft 365
trust
eduGAIN
InCommon
SSO login
trust
Saas applications
Entra ID
cloud
sync
datacenter
trust
trust
Entra Connect
trust
Datacenter applications
Key
Federation trust
Credential validation/attribute lookup
Object sync
sync
authN / attributes
Shibboleth IdP
Active Directory


SMU
2025
Microsoft 365
trust
eduGAIN
InCommon
SSO login
trust
Entra ID
Saas applications
cloud
sync
datacenter
SAML proxy
trust
Entra Connect
trust
Datacenter applications
Key
Federation trust
Credential validation/attribute lookup
Object sync
sync
attributes
Shibboleth IdP
Active Directory

2025 architecture description

		2024 (before)	2025 (after)
Active Directory			
	single domain	yes	yes
	enterprise directory service	yes	yes
SSO service			
		Shibboleth IdP	**Entra ID**
Entra ID			
	Entra Connect for sync	yes	yes
	authentication source	**Shibboleth IdP**	**Entra ID (direct)**
Shibboleth IdP			
	authentication source	**Active Directory (direct)**	**Entra ID (proxy)**
	attribute resolver	Active Directory	Active Directory
	local SAML SPs	~100	~100
	total SAML SPs	~300	~300
Duo integration			
		Shibboleth IdP	**Entra ID**

Technical references

SAML Proxy

SAML Proxying EntraID / Azure with the Shibboleth IdP - Shibboleth Knowledge Base - Confluence

Solution 2: Microsoft Entra ID with Shibboleth as a SAML proxy - Microsoft Entra | Microsoft Learn

Password Hash Sync (PHS)

Implement password hash synchronization with Microsoft Entra Connect Sync - Microsoft Entra ID | Microsoft Learn

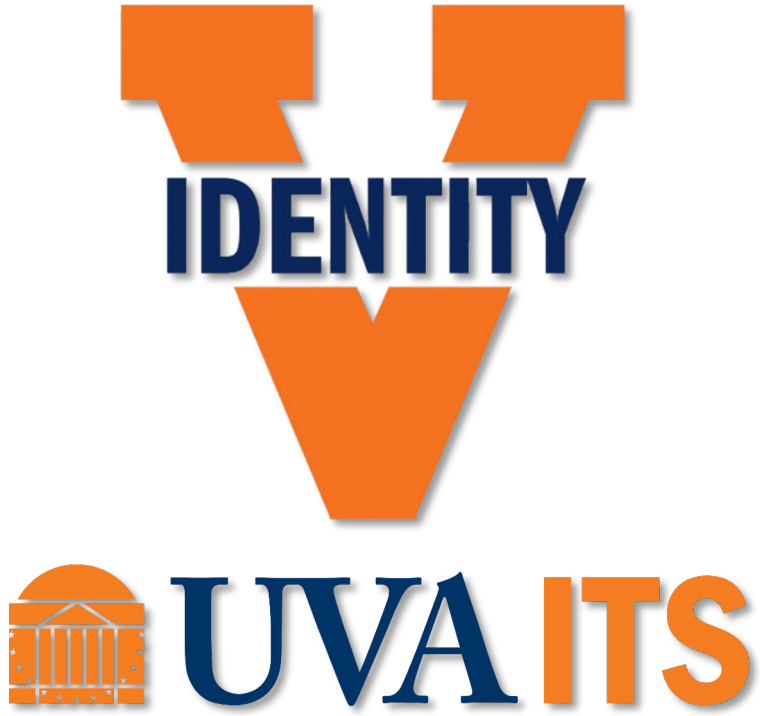
PHS Staged rollout

Microsoft Entra Connect: Cloud authentication via Staged Rollout - Microsoft Entra ID | Microsoft Learn

University of Virginia

Where We Are Now

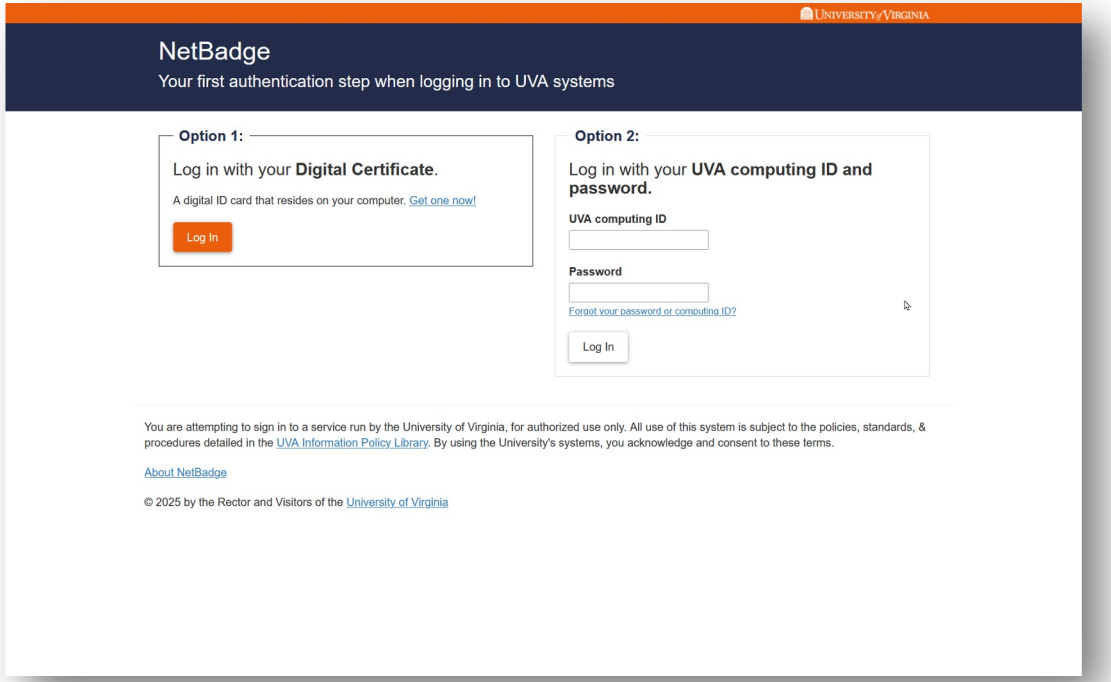
- Identity Services – Fischer IGA, Grouper, Shibboleth (as of Feb 2025)
  - Engineering
    - 1 Manager
    - 3 Solution Engineers
    - 1 DevOps Engineer
    - 1 Architect
  - Operations
    - 1 Manager
    - 3.5 Business Analysts
  - Access Management (reporting through Support Services & Learning Technology Group)
    - 1 Manager
    - 5 Support Technicians



- 30k Students
- 5k Faculty
- 24k Staff
- 1.25M Total Identities w/ 19 Primary Roles

A Quest for “Single” Single Sign-On

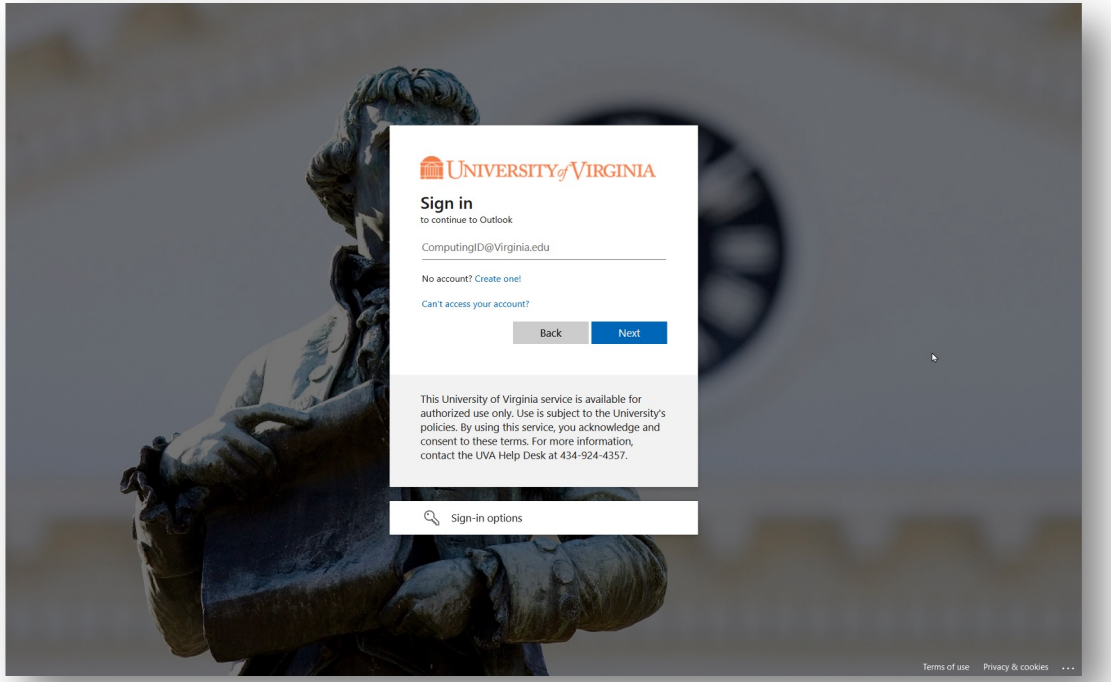
- Deployed Shibboleth IdP v5
  - Branded as NetBadge
  - Approx. 750 SAML Integrations (many InCommon)
    - Most **major** applications, including:
      - Workday
      - Zoom
      - PeopleSoft SIS
      - Box
      - Canvas
  - Three authentication sources (via JAAS)
  - Cisco Duo for MFA.
  - Integration Requests through ServiceNow



https://in.virginia.edu/netbadge

A Quest for “Single” Single Sign-On (Con’t)

- Deployed Entra ID
  - Main application: Office 365
    - Primary Email for Students, Faculty, Staff
  - Approx. 600 SAML Integrations
    - Many one-off applications and ad hoc integrations
    - Internal ITS Applications (LogicMonitor, Splunk)
    - Everything OAuth 2.0 / OpenID Connect
  - One authentication source: Active Directory
    - Approx. 90k Users
  - Cisco Duo for MFA.
  - No clear governance model.
  - No clear inventory.



Why are we going there? SSO Perceptions

There is a very real view in the broader identity space that Shibboleth is a legacy platform and that Microsoft Entra is the future.

“Our peer institutions are embracing Entra…”

“We’re already paying for it…”

“Microsoft is innovating in the identity space…”

What solution or solutions are right for UVA?

Cards on the Table: SSO Options for UVA

- Going “All In” on Shibboleth
- Going “All In” on Entra ID
- Taking Hybrid Approach
- Something Else Entirely

SSO Options for UVA

- ~~Going "All In" on Shibboleth~~
- Going "All In" on Entra ID
- Taking Hybrid Approach
- Something Else Entirely

Realistically this is just not happening:

- Entra is deeply embedded…
- Too many people like it…
- There's no real institutional desire to give up on it…

There are too many good things about Entra to even seriously entertain this option.

SSO Options for UVA

- Going “All In” on Shibboleth
- Going “All In” on Entra ID
- Taking Hybrid Approach
- Something Else Entirely

- Multilateral Federation (InCommon)
  - Do we just buy Cirrus Bridge?
- Entity Migration
  - How many hours to curate and implement?
- User Population Reconciliation
  - How many additional users need to be surfaced into Azure AD?
- Governance
  - Inventory
  - Policies
  - Procedures

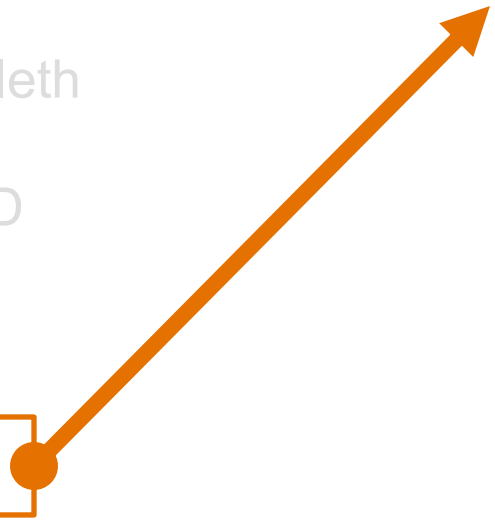
SSO Options for UVA

- Going “All In” on Shibboleth
- Going “All In” on Entra ID
- Taking Hybrid Approach
- Something Else Entirely

- **Proxy one IDP to Another!**
  - Which IDP is Primary?
- Multilateral Federation (InCommon)
  - Again, do we just buy Cirrus Bridge?
- Entity Migration
  - Again, how many hours to curate and implement?
- User Population Reconciliation
  - Do any additional users really **need** to be surfaced into Azure AD?
- Governance – what does a hybrid framework look like?
  - Do we even try to implement a combined policy?

SSO Options for UVA

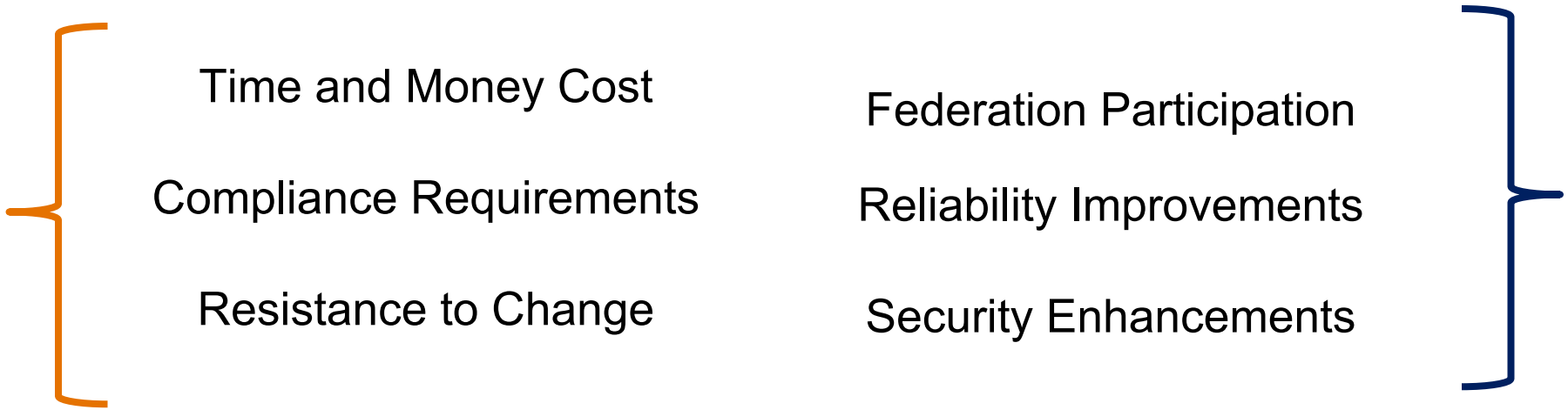
- Going “All In” on Shibboleth
- Going “All In” on Entra ID
- Taking Hybrid Approach
- Something Else Entirely



- **What “else” exactly?**
  - “Complex” Proxying
    - Custom Authentication Flows
    - Handling Certificate-based Authentication
  - Keep ‘em Separated
    - Address Governance of Entra RPs
    - RP-Specific Authentication Needs Dictate
    - Slow Migration to Entra?
    - Begin Leveraging Advanced Entra Features
      - Passwordless
      - B2C Guest Access
  - Ping? Okta?

So… what advice do we have?

- UVA is still early on our quest for a “single” single sign-on solution…
- Sharing in this journey with the community so that we all benefit from this hard work!
- Our (broad) considerations:



Let’s Discuss

Q&A

Q & A

We’re taking questions and comments live using the Zoom Q&A function.

Want to Continue the Conversation?

Closing

June 2 - 6, 2025

Register Now: https://incommon.org/academy/camp-meetings/basecamp/

Buy 2 Get 1 - Bring your Team

BaseCAMP

- Identity Management Fundamentals
- Intro to InCommon and the Trusted Access Platform components
- Understanding and Building IAM Initiatives
- Federation Basics
- Grow Your Network and Get Connected!

5 (half day) virtual event

Trusted Access Platform Component Training

FEB	MAY		AUGUST	SEPT	OCT	NOV
Shibboleth Feb 24-28			**UPDATED: Grouper Core Training**			
	midPoint Multi-Affiliations Training Early May **NEW**	**Grouper** Live Training Practical Application (May)	**Grouper** Live Training Practical Application Aug 6-8	**Shibboleth** Mid Sep	**midPoint** Multi-Affiliations Training Mid Oct **NEW**	**Grouper** Live Training Practical Application Nov 18-20

COmanage Expression of Interest: We have a community-activated option to help transform your team's learn COmanage. We'll create a dedicated training experience when you're ready. Fill out this form to let us know you're interested!

Learn more here: https://incommon.org/academy/software-training/

Shibboleth® Grouper™ COmanage™ midPoint

THANK YOU

Thoughts about today's program?

Please complete our Zoom survey.

Feedback about IAM Online?

Contact Jean Chorazyczewski, jeanc@internet2.edu

Got Ideas?

Submit your ideas for future IAM Online webinars!
www.incommon.org/academy/iamonline/iamonline-ideas

Next IAM Online: April 16, 2025

Strategies for Cross-Institutional Course Sharing

As student enrollment declines, institutions are turning to course-sharing to expand offerings without significant costs. But balancing access for students, faculty, administrators, and IT teams presents challenges. The Interactive Distance Education Alliance (IDEA) and InCommon have partnered to develop a federated identity solution—engaging 20 institutions and 30+ stakeholders to streamline access across learning management systems. This initiative removes login barriers, enabling seamless multi-institutional course registration. Join us to explore how InCommon Federation simplifies SSO for course-sharing, library resources, and more!