



cirrus identity

www.cirrusidentity.com

Cirrus Proxy Webinar

Learn about the Cirrus Identity Provider Proxy!

Hear directly from Cirrus customers on how they simplified SSO for multiple institutions with the Proxy cloud solution!

Your Swiss Army Knife of Simple and Secure Login Solutions

for higher education and enterprise

<https://www.cirrusidentity.com>

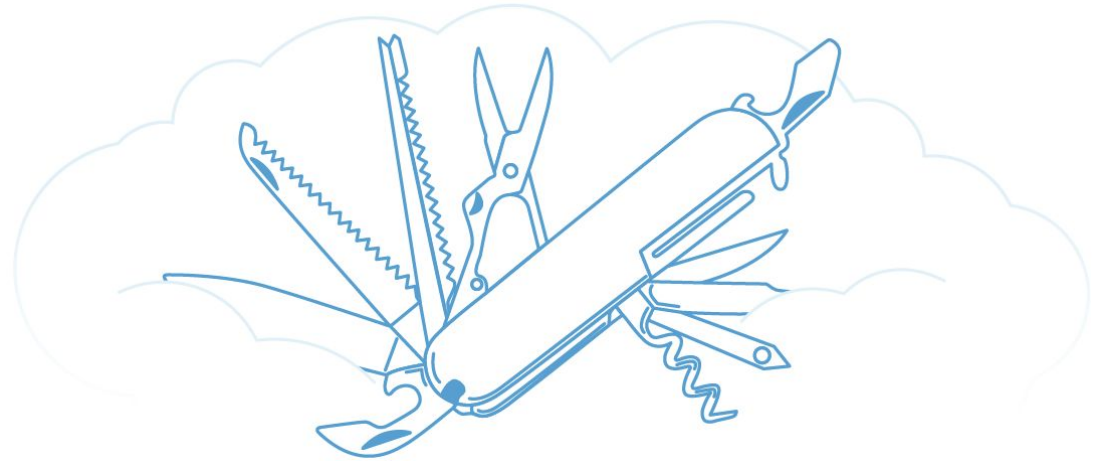
Welcome & Introduction!

By Dedra Chamberlin

Cirrus Identity CEO & Founder

Who is Cirrus Identity?

Your Swiss Army Knife for
Digital Identity Management



2022 Webinar Series

Past:

- [Cirrus Identity Bridge](#) - Connect Azure AD and Okta to InCommon



Upcoming:

- Social and OrgBrandedID Login - Solutions for Alumni and Online Learning



Focus for Today's Webinar



Cirrus Identity Provider Proxy

Webinar Goals

1. Share higher ed trends and why institutions are using the Cirrus Proxy solution
2. Explain more about Proxy functions and implementation considerations
3. Hear implementation stories from Cirrus Proxy customers

Agenda & Introductions

1. **Cirrus Proxy Institutional Drivers & Key Features - Mark Rank, Director of Product, Cirrus Identity - 10 min**
2. **Proxy Functions & Considerations - Patrick Radtke, Chief Technology Officer, Cirrus Identity - 10 min**
3. **Cirrus Bridge Customer Panel - 15 min**
 - a. **Todd Robinson** - Enterprise Technology Architect, Duke Clinical Research Institute
 - b. **Whinston Antion** - Assistant Director, Identity & Access Management, West Virginia University
4. **Open Forum Questions & Answers - 20 min**

Cirrus Proxy: Institutional Drivers & Key Features

By Mark Rank

Cirrus Identity Director of Product

Institutional Drivers

Driver #1: User Experience!

Some of the things Cirrus hears:

- Our <<insert important professional school>> issues their own accounts but needs to access some central services
- Medical staff from our affiliated hospital system need access to our academic library resources
- Research staff from other institutions need access to our applications
- There are # institutions in our university system and each institution needs easy access to shared applications



**Driver #2:
Organizational
Resources!**

Some of the things Cirrus hears:

- We have an executive that keeps asking “Why are we running this, isn’t there a cloud solution?”
- Individual campuses can better support their end user account access, but we need everyone to access some shared services
- There are limited staff to run access management services for multiple institutions or a system office



Driver #3:

Technical Flexibility!

Some of the things Cirrus hears:

- The vendor only supports one SAML IdP, but we need to integrate two different ones
- The service provider only supports CAS, but we need to integrate two different identity providers and use a discovery service
- We have users from <<insert number from 2-2000>> institutions, and we need them to all access a collection of <<insert number from 5-50>> services
- We want to require sponsorship, select a profile, check an identity, or add attributes to the incoming SAML assertion



High Level Architecture & Key Features

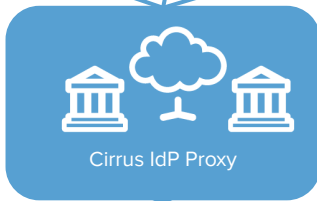
Multilateral Federation

Service Providers

Application #1

Application #2

Application #3



Identity Providers

Institution #1



Institution #2



Institution #3



Institution #4



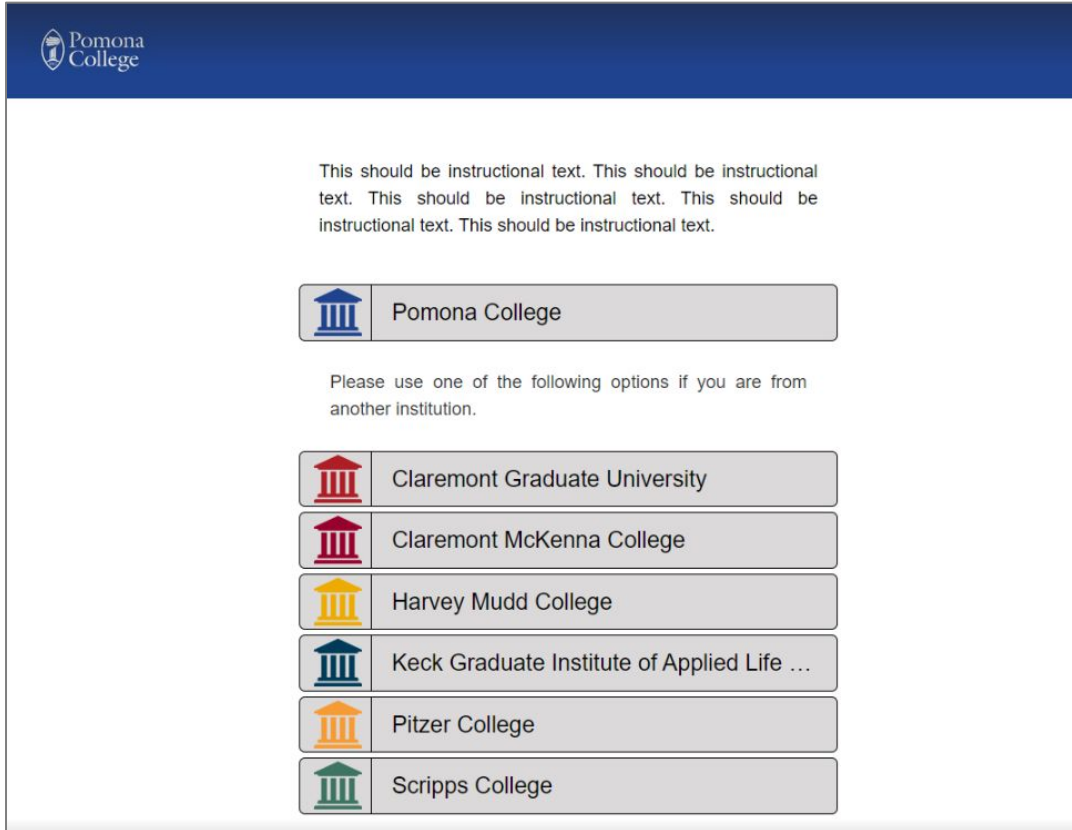
Institution #5



Shared Metadata




Customer Login Discovery





Pomona College


This should be instructional text. This should be instructional text. This should be instructional text. This should be instructional text. This should be instructional text.


 Pomona College


Please use one of the following options if you are from another institution.


 Claremont Graduate University

 Claremont McKenna College

 Harvey Mudd College

 Keck Graduate Institute of Applied Life Sciences

 Pitzer College

 Scripps College

Multilateral Federation & Protocol Translation

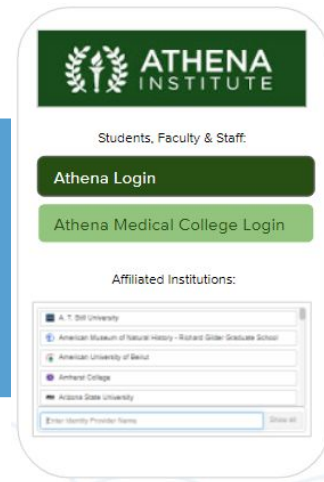
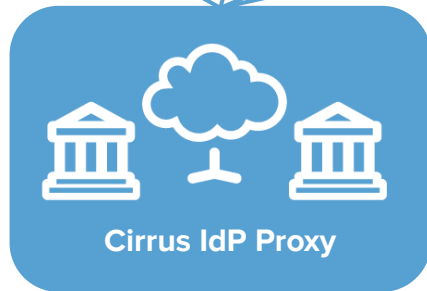
Service Providers

CAS App(s)

SAML App(s)

OIDC App(s)

WS-FED App(s)



Identity Providers

Institution #1



Institution #2



Institution #3



Institution #4



Institution #5



Policy Enforcement

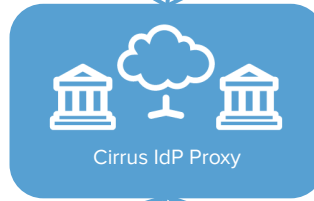
Service Providers

Application #1

Application #2

Application #3

Policy Enforcement
(Require MFA, Sponsorship, or Certain Attributes)



Identity Providers

Institution #1



Institution #2



Institution #3



Institution #4



Institution #5

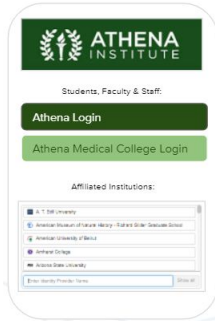


Cirrus Account Linking

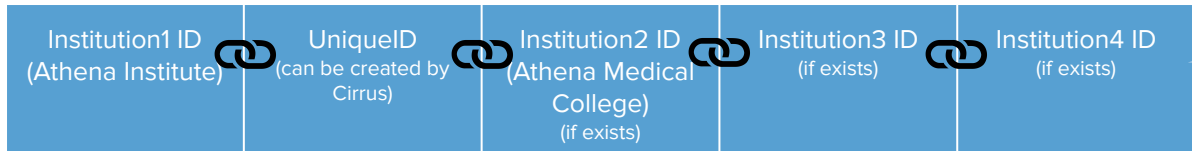


#3 Cindy can access all the systems that Athena Medical College has access to

Business Logic in the Cirrus Proxy
Asserts the ID that each application is expecting based on successful authentication



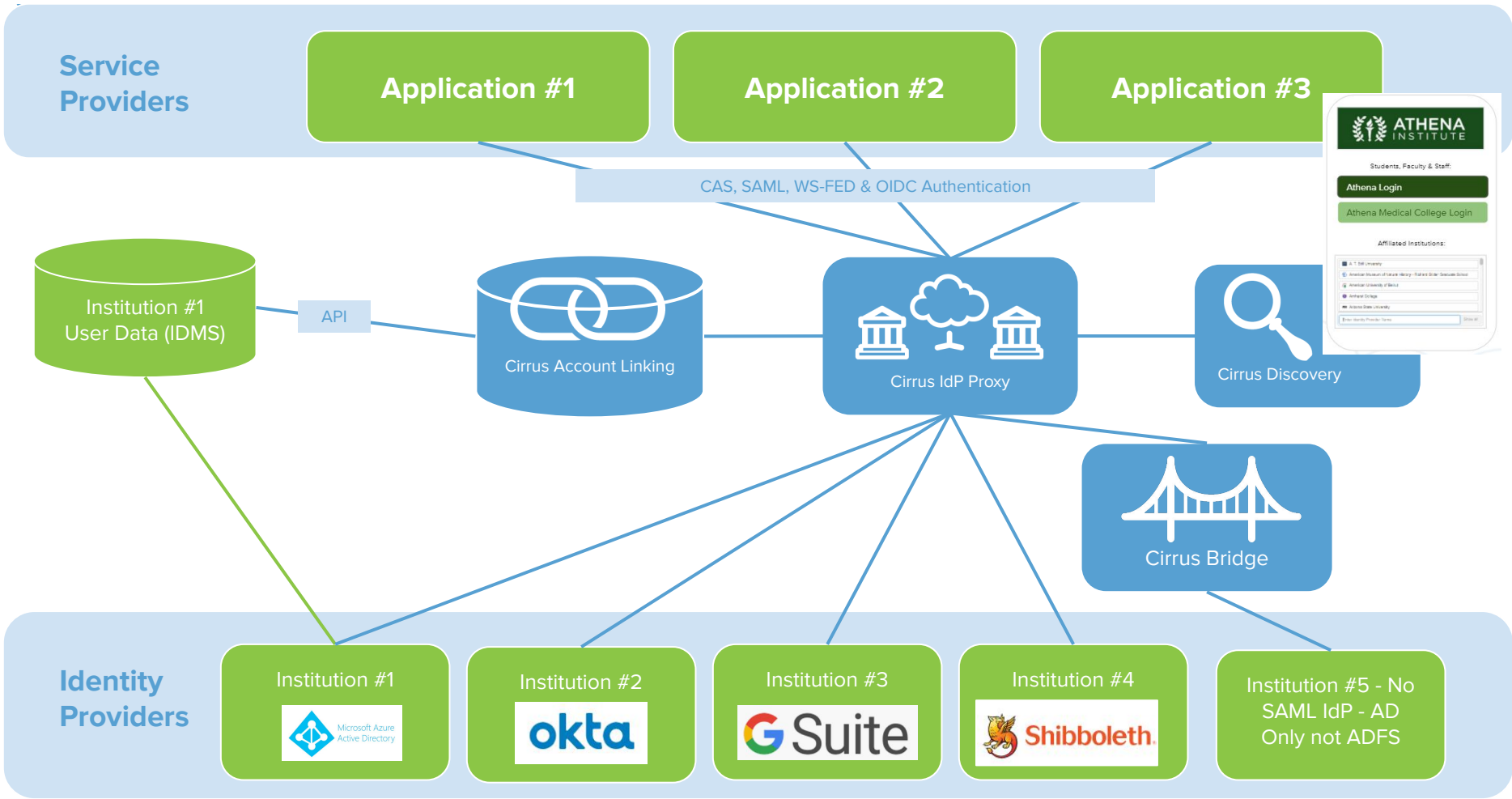
#2 Cindy selects her institution and authenticates with her username and password



#1 Cindy can have multiple IDs, which are linked by Cirrus

Cirrus Account Linking Database
Links identifiers and/or attributes from multiple institutions

Cirrus Proxy Solution Architecture



Cirrus Identity - Identity Provider Proxy - Key Features

Base Proxy

- Integrates with any SAML V2, CAS, or OIDC identity provider – including the Cirrus Bridge or Cirrus OrgBrandedID
- Acts as an Identity Provider to configured Service Providers
- Provides SAML, CAS, or OIDC authentication incoming or outgoing
- May be configured to only trust a small subset of SPs and IdPs, as determined by the institution
- Consumes metadata dynamically from eduGAIN federations, including InCommon, on a daily basis for new or changed SPs or IdPs
- Supports REFEDS authentication context signalling
- Can be registered as either an SP or IdP in eduGAIN federations
- Supports flexible attribute release



Discovery Service

- The Discovery service login screen is included as an option at no extra charge.
- The Discovery interface has many styling properties to customize and brand the login screen for the institution.

Additional Options

- Support for custom metadata aggregates or custom attribute release policies.
- Integration with:
 - Cirrus Account Linking
 - Cirrus Gateway
 - Cirrus OrgBrandedID
 - Cirrus Invitation
 - Cirrus MFA
- Support for external attribute authorities

Cirrus Identity - Identity Provider Proxy - Value

			
<p style="text-align: center;">Improve User Experience</p> <ul style="list-style-type: none"> Streamline the SSO login process for all institutional users. Provide faster access to systems, reduce frustration and provide a positive user experience. 	<p style="text-align: center;">Maximize Federated Services</p> <ul style="list-style-type: none"> Maximize investments in shared/federated services Support secure access from affiliated or federated organizations. Users can login with their institution's username and password to access applications! 	<p style="text-align: center;">Reduce Operating Expense</p> <ul style="list-style-type: none"> Retire costly legacy infrastructure. Save both IT and service desk labor expenses. Refocus resources on other top priorities! 	<p style="text-align: center;">Reduce Technical Risk</p> <ul style="list-style-type: none"> Utilize professionally managed cloud services for higher ed. Reduce technical risk for legacy systems. Shore up IAM team resources. Improve business continuity for mission critical systems.

Cirrus Identity is a **Trusted** InCommon Catalyst Partner



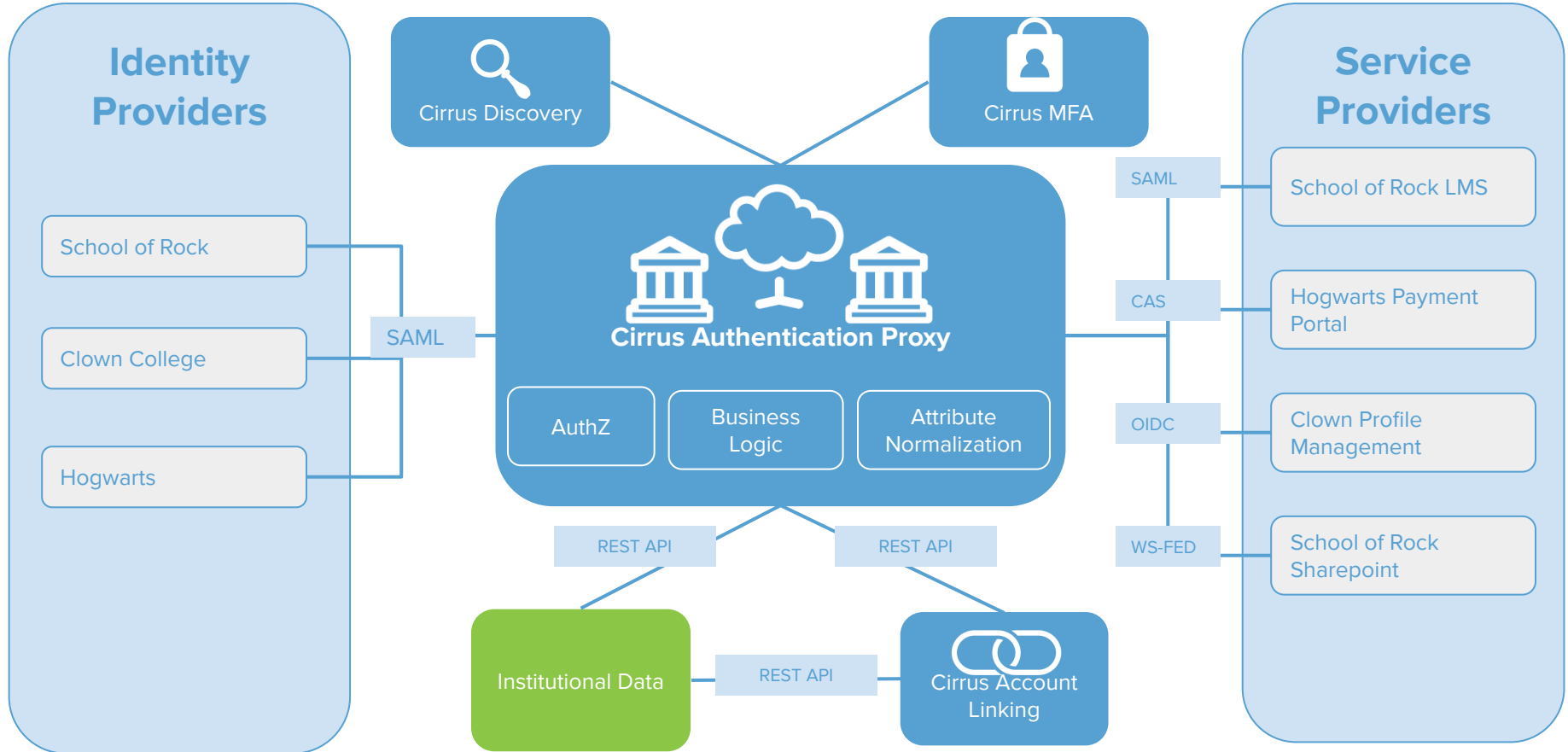
Proxy Features & Considerations

By Patrick Radtke

Cirrus Identity CTO

What is an Authentication Proxy?

A proxy sits in the middle of authentication requests and responses to provide additional functionality and/or protocol translation.



General Proxy Functions

Provides functionality that either the IdP or SP cannot provide on its own.

Makes a heterogeneous mix of IdPs or SPs appear homogeneous.

General Functions:

- Protocol Translation (SAML2, CAS, OIDC, WS-FED)
- Attribute normalization
- Authorization control
- Attribute decoration (often integrated with Cirrus Account linking module)
- Conditional MFA
- Business logic

Enabling 1 to many

- Many service providers only support one Identity Provider.
- Higher ed and research institutions commonly have the need for multiple IdPs to have access to applications.
- Sometimes a service is composed of lots of changing service providers. Registering each into a federation and getting attributes released is a pain point.

Considerations for Implementing a Proxy Solution

- Create an attribute map
- How will provisioning and authorization be handled in your applications
- Proxy handles authentication and signing for all users. Keep it secure
- Some SaaS products require you to control the email domain of the users
- Scope checking happens at the proxy
- InCommon and picking an entityID

Cirrus Customer Panel

Todd Robinson

Enterprise Technology Architect, Duke Clinical Research Institute

Researchers Access to Sharepoint Use Case



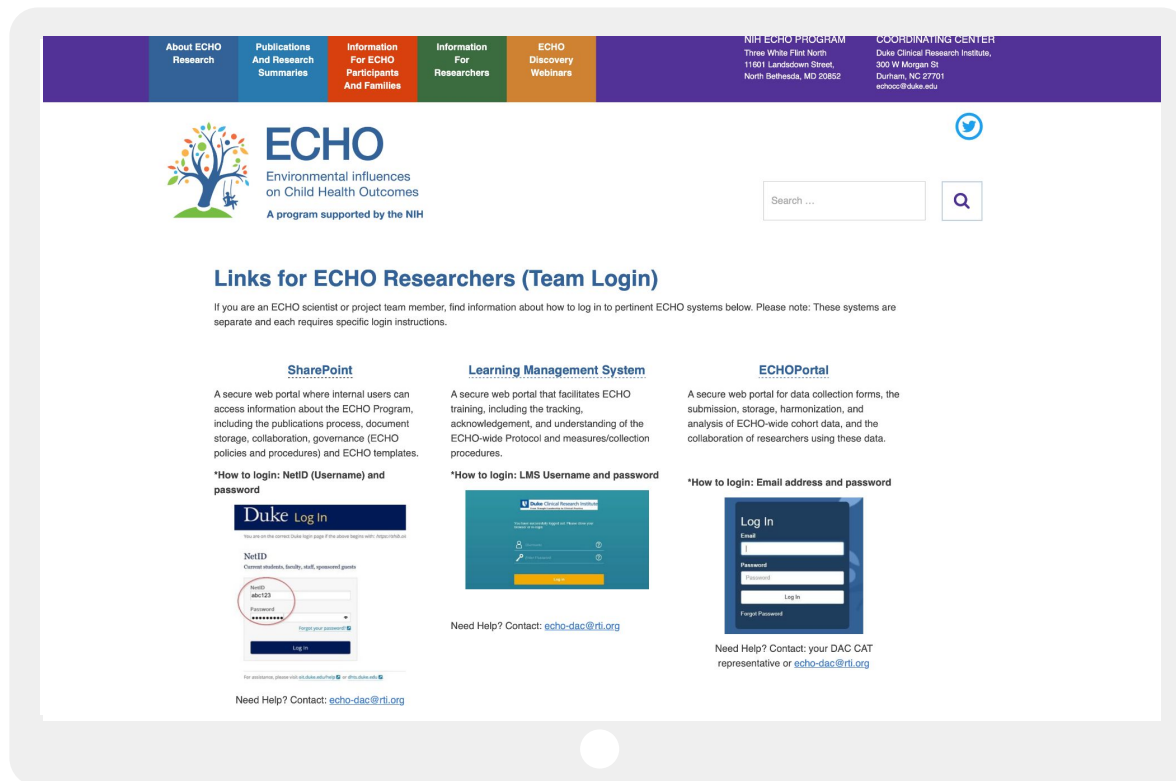
Background

- DCRI needed a way to allow users to access solutions without requiring them to create Duke accounts
- Providing Single Sign On (SSO) functionality was desired
- Users did not want another account to manage
- Our risk management team wanted us to reduce the number of sponsored accounts
- The Cirrus Identity Provider Proxy easily incorporates the InCommon Federation which allowed 80% of the users to leverage their organizational accounts
- The User Interface for managing the Proxy makes changing the look of the Discovery Service and the list of institutions users can choose from a breeze

Researchers visit ECHO site

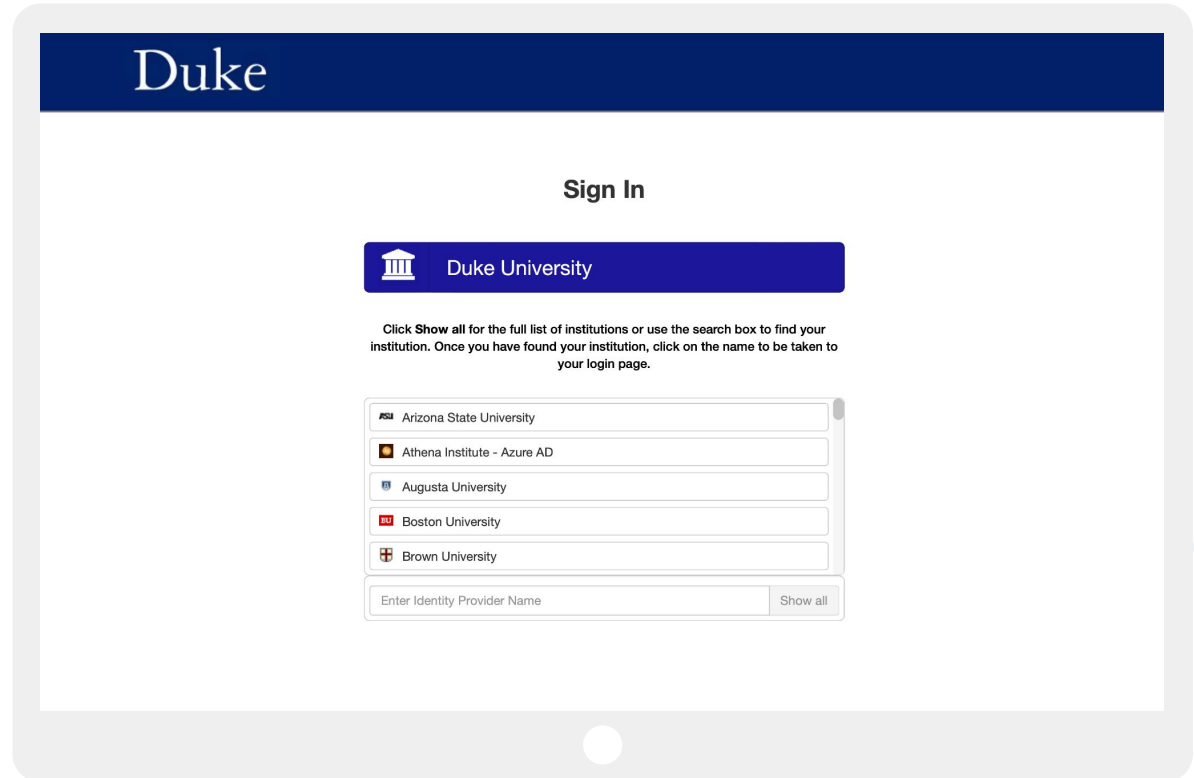
They can choose from 3 SPs

Sharepoint is integrated with the Cirrus Proxy



Users choose a login provider

DCRI staff can easily add new IdPs to the list of options via the discovery service config panel in the Cirrus console



Implementation Highlights

- SharePoint had to be configured to use the Cirrus Identity Provider Proxy rather than the Active Directory for Authentication
- Using the Proxy allowed DCRI to configure a single Identity Provider rather than each institution's
- We needed a solution implemented inside of 3 months
- Cirrus' experience with InCommon was invaluable and handled registering with the federation
- Since SharePoint works with WS-FED claims instead of SAML assertions, Cirrus helped make the conversion so users would authenticate using SAML but SharePoint would get a claim

Lessons Learned

- The biggest challenge was around User Profiles in SharePoint and migrating the users from Active Directory to the corresponding new identifier
- An issue with Office integration caused some issues that Cirrus helped us work through although it was not a Cirrus issue
- A test site that displays the information in the assertion is a great tool to verify the organization is releasing the needed attributes. This is now part of our onboarding process for a new organization

Whinston Antion

Assistant Director, Identity & Access Management, West Virginia University

Hospital, K-12 and Alumni Use Case



- **Multiple authorized user populations need access to select WVU resources, but....**
 - Hospital users are not in our directory
 - State high school students from specific counties are not in our directory
 - Dues Paying Alumni are in our directory, but not actively licensed
 - Bonus round: Parents aren't consistently in **any** directory
- **Why was Cirrus selected? ... “Federation” from a single login screen using:**
 - SAML Proxy Service
 - Account Linking & ID Verify Services
 - Invitation & Org-branded ID Services
 -more

Account Association Overview

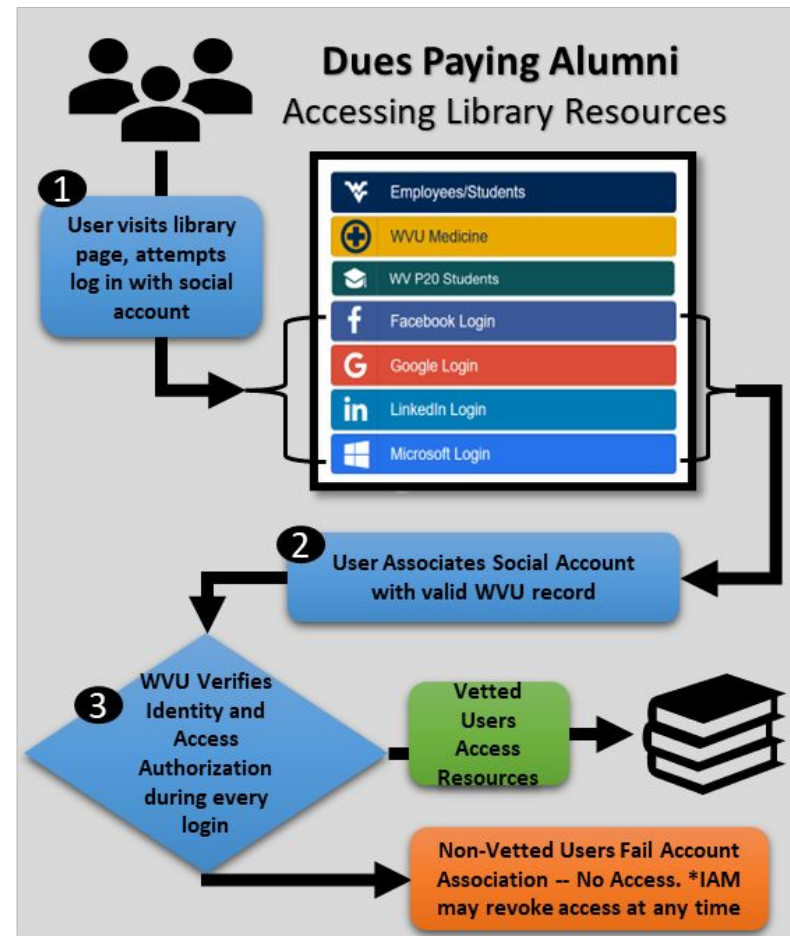
Select WVU populations may use their Social Media Accounts to login to authorized resources. Dues Paying Alumni are currently able to login using their social accounts.

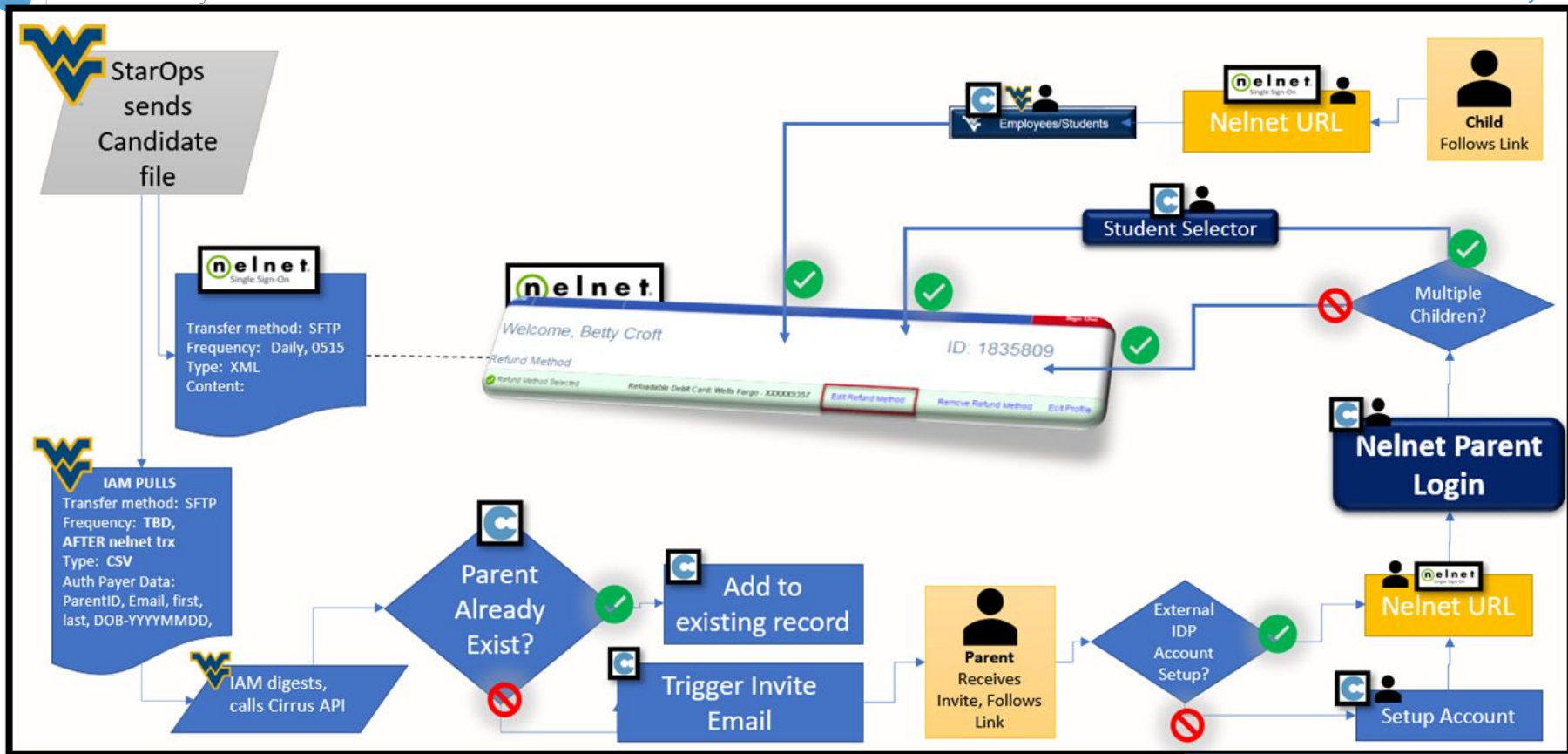
How does it work?

- WVU Identity and Access Management (IAM) maintains record of all students and employees in the Identity Repository. When a user associates a Social Media Account, they must provide proof they are a WVU Dues Paying Alumni/Retiree.
- IAM **verifies** the proof and decides if account association is authorized based on the user's WVU record in the identity repository. WVU resources may have additional controls to prevent or allow access based on user attributes.
- The vetted person may then log in, using their associated and verified social media account. From the WVU system perspective, an approved WVU user is logging in, not a social media account.

Whinston Antion

Assistant Director, Identity & Access Management





Lessons Learned

- Business needs *sometimes* deviate from OOTB
- Org-Branded IDP is a valuable addition to our IAM toolbox
- Cirrus provided consultation, new service development, and delivery in a tight timeline

Questions & Answers

Stay Tuned for More Webinars!



If you would like to hear more about the Cirrus Proxy,
please email sales@cirrusidentity.com!



cirrus identity

Dedra Chamberlin,
CEO
dedra@cirrusidentity.com

Mark Rank,
Director of Product
mark.rank@cirrusidentity.com

Patrick Radtke,
CTO
patrick@cirrusidentity.com

Kristina Deaton,
Director of Customer Success
kristina@cirrusidentity.com

Karen Kato,
Director of Sales & Marketing
karen@cirrusidentity.com