



**cirrus** identity

# Attribute Authority Webinar

**Welcome!**

**Dedra Chamberlin**  
**CEO**

# Welcome!

- Who is Cirrus Identity?

## Attribute Authority Webinar Agenda

- Introduction to the Cirrus Identity Attribute Authority - **What is it? What does it enable? How is it Implemented?**
- Attribute Authority Technology - **Authentication Flow & Data Timeliness**
- Customer Presentation - **Angelo State University**
- Customer Presentation - **SUNY Geneseo**
- Questions & Answers

Please mute yourself until Q&A and feel free to enter comments/questions into Zoom chat

# Cirrus Attribute Authority Introduction

Mark Rank  
Director of Product

# What is it?

1. A Cirrus hosted solution that enables real time integration of additional attributes not contained in the initial authentication assertion
2. Source can be either LDAP enabled directories, or a REST API (based on Cirrus specs) to enabled data sources
3. Integrates with either the Cirrus Bridge or Cirrus Proxy
4. Also meets the requirements to be used directly with Entra ID (fka Azure AD) Custom Claims Providers

# Cirrus Attribute Authority enables:

- a. Including sensitive attributes in SSO assertions that are not allowed in commercial Web SSO solutions (Entra ID, Otko, or others)
- b. Organizations with highly customized directories to migrate to commercial Web SSO solutions
- c. Accelerating the migration of organizations to commercial Web SSO solutions without needing to migrate all the attributes
- d. Augmenting SSO assertions for service providers behind a Cirrus Proxy

# How is it implemented?

1. Direct integration with Cirrus Bridge for Entra ID, Okta, or other commercial Web SSO solutions
2. Using Microsoft Entra ID (fka Azure AD) Custom Claims Provider functionality
3. Direct integration with Cirrus Proxy
4. LDAP requires service account, query parameters and firewall access

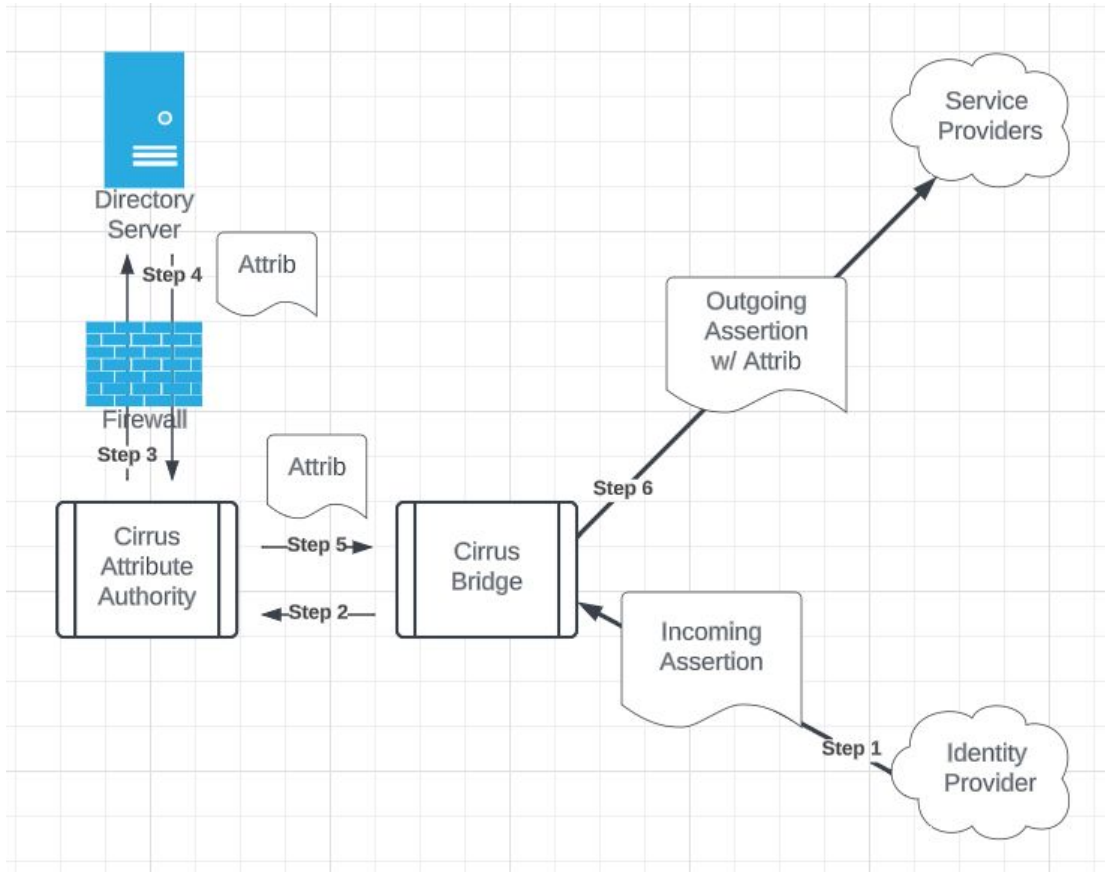
We will see #1 and #2 when we review our customers



# Cirrus Attribute Authority Technology

**Mark Rank**  
Director of Product  
**Patrick Radtke**  
CTO





## Authentication Flow

1. Entra Id / Okta provide incoming assertion
2. Bridge makes request to AA
3. AA queries target directory server
4. Directory server returns additional attribute(s)
5. AA responds to Bridge with requested attributes
6. Bridge adds attributes to original assertion based on the configuration and sends to service provider

# Data Timeliness

1. Cirrus Attribute Authority is not a data syncing tool
2. The Attribute Authority is retrieving the data in real time from the data source
3. The asserted attributes are as up-to-date as the source system is
4. The only constraint is on the authentication session time

# Cirrus Identity Customer Presentations



**GENESEO**  
THE STATE UNIVERSITY OF NEW YORK

# Customer Presentations:

1. What was your organization's challenge?
2. Review of the institution's before & after architecture and implementation
3. Advice and/or lessons learned

Questions will be taken after Both Presentations

# Angelo State University Introductions



# Angelo State Challenge:

- Angelo State was running WS02 for CAS & SAML. CAS was limping along. ASU wanted to consolidate on Azure AD and utilize the Cirrus CAS and SAML Bridges.
- The ASU Campus ID was classified as sensitive data and needed to be removed from the directory and could not be in Azure AD where it could be exposed.
- The Campus ID comes from Banner and is loaded into LDAP as a protected schema extension.
- A handful of ERP applications needed the Campus ID for authentication since it is an immutable ID and email is not - Angelo State allows name changes.
- ASU had never set up InCommon Federation although it was requested from Grants Office for 4-5 years for access to NIH and NSF research.gov.

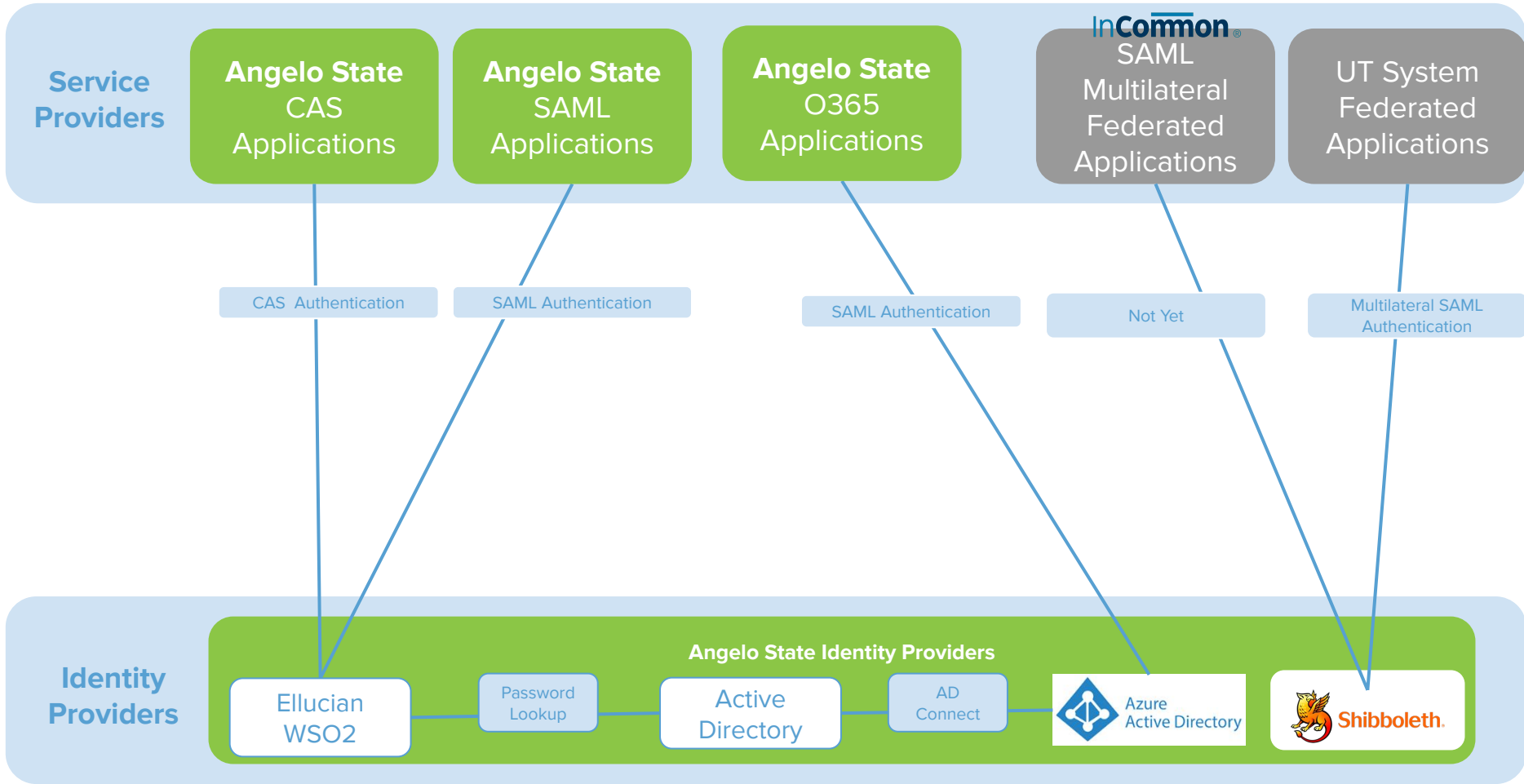


# Angelo State University & Cirrus Implementation Overview





# Angelo State - Before Cirrus Bridge & Attribute Authority



# Angelo State - **After** Cirrus Bridge

**Service Providers**

**Angelo State CAS Applications**

**Angelo State SAML Applications**

**InCommon® Federated SAML Applications**

**UT System Federated SAML Applications**

CAS Authentication

SAML Authentication

Multilateral SAML Authentication

Retired Ellucian WSO2 - CAS

**Cirrus CAS Bridge**

Retired Ellucian WSO2 - SAML

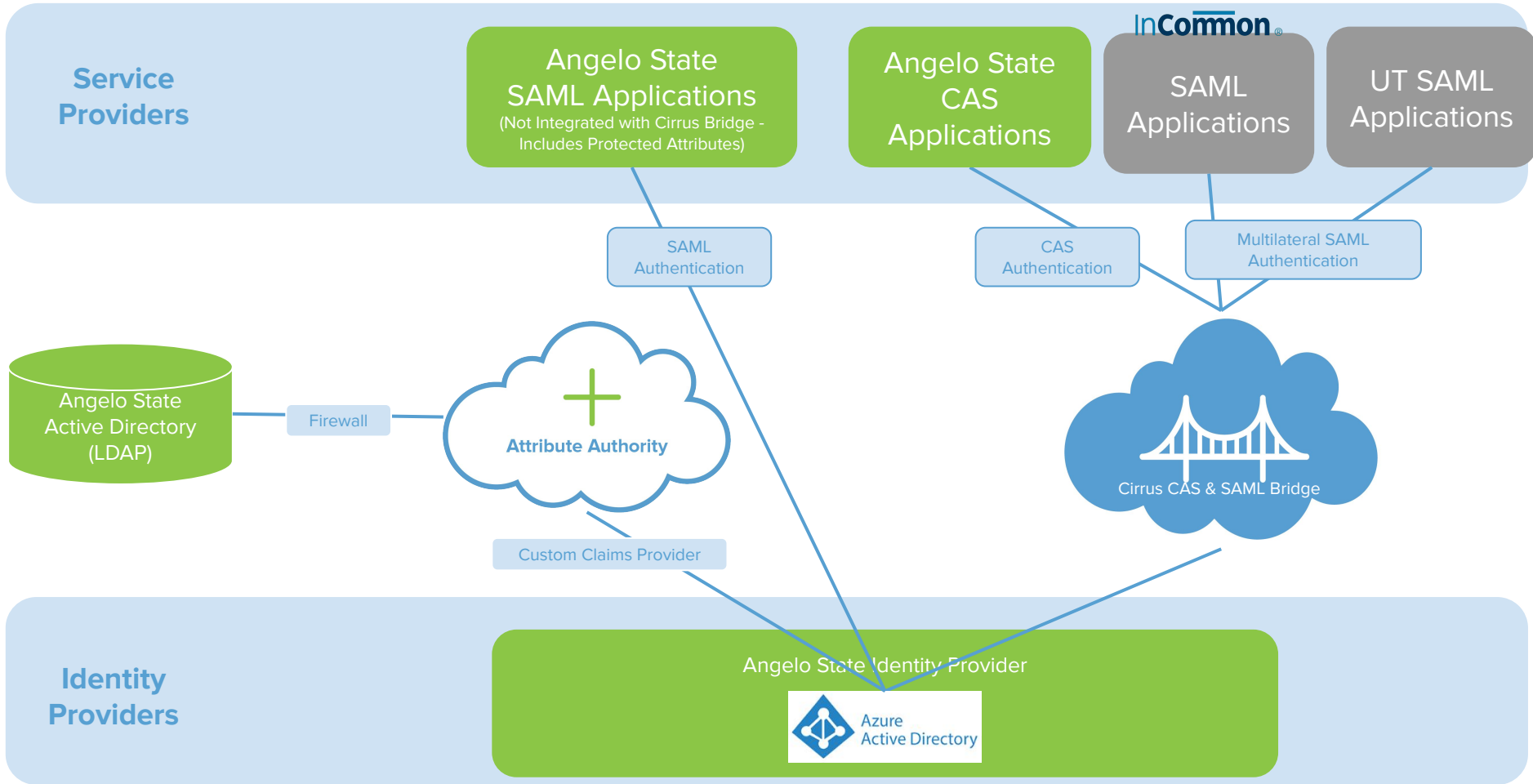
**Cirrus SAML Bridge**

**Identity Providers**

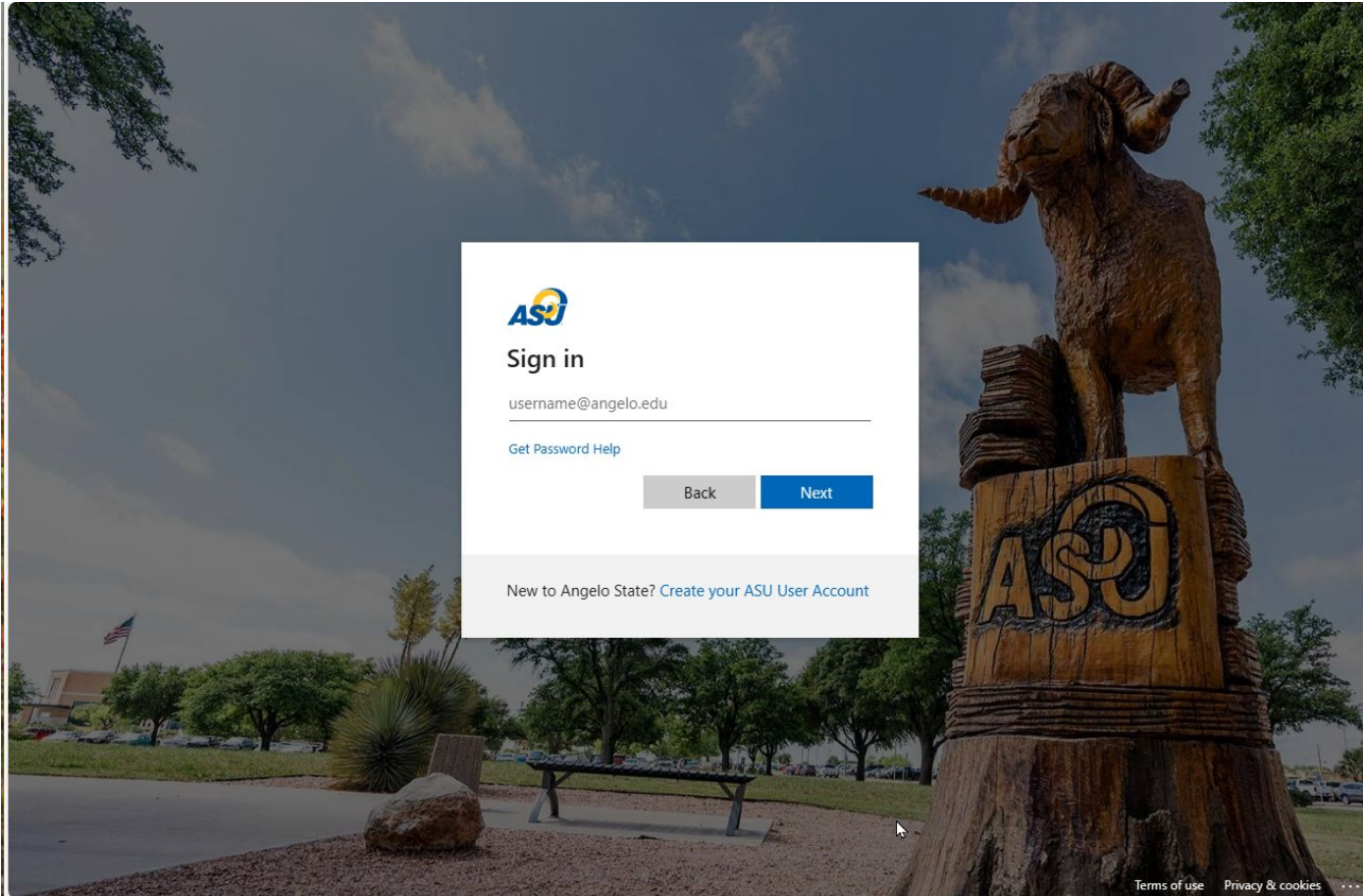
**Institution's Identity Provider**



# Angelo State - **After** Cirrus Attribute Authority



# Angelo State Login Screen - All Applications



# Advice & Lessons Learned:

- We investigated Microsoft Custom Security Attributes, but they're not available as enterprise app claims, nor easily populated.
- Azure AD Schema Extensions via AD Connect are exposed within MS Graph v2 user profile, falling short of our attribute security requirements.
- Service Provider Inventory can be challenging and may require multiple review iterations.
  - Export all
  - Assess utilization
  - Clean/Correct/Normalize
  - Document claims on minimized list
- Around 30% of our apps were SAML under the same hostname and software as CAS services. The DNS cutover would have been very convenient if there was less SAML presence.

# State University of New York, Geneseo Introductions



**GENESEO**  
THE STATE UNIVERSITY OF NEW YORK

# SUNY Geneseo Challenge:

- Azure AD had been identified as the primary Identity Provider. CAS and SimpleSAMLPhp (SSP) were integrated with Azure AD, but aging.
- CAS was hosted on-prem and due for an upgrade which had been delayed.
- SSP was used to support multilateral federation with Azure AD and it was one more piece of the IAM environment that needed to be maintained.
- The employee number (G number) and employee type were stored in LDAP and required for authentication for some applications. They are both protected attributes and could not be loaded into Azure AD because it lacks support to meet the Geneseo privacy needs.

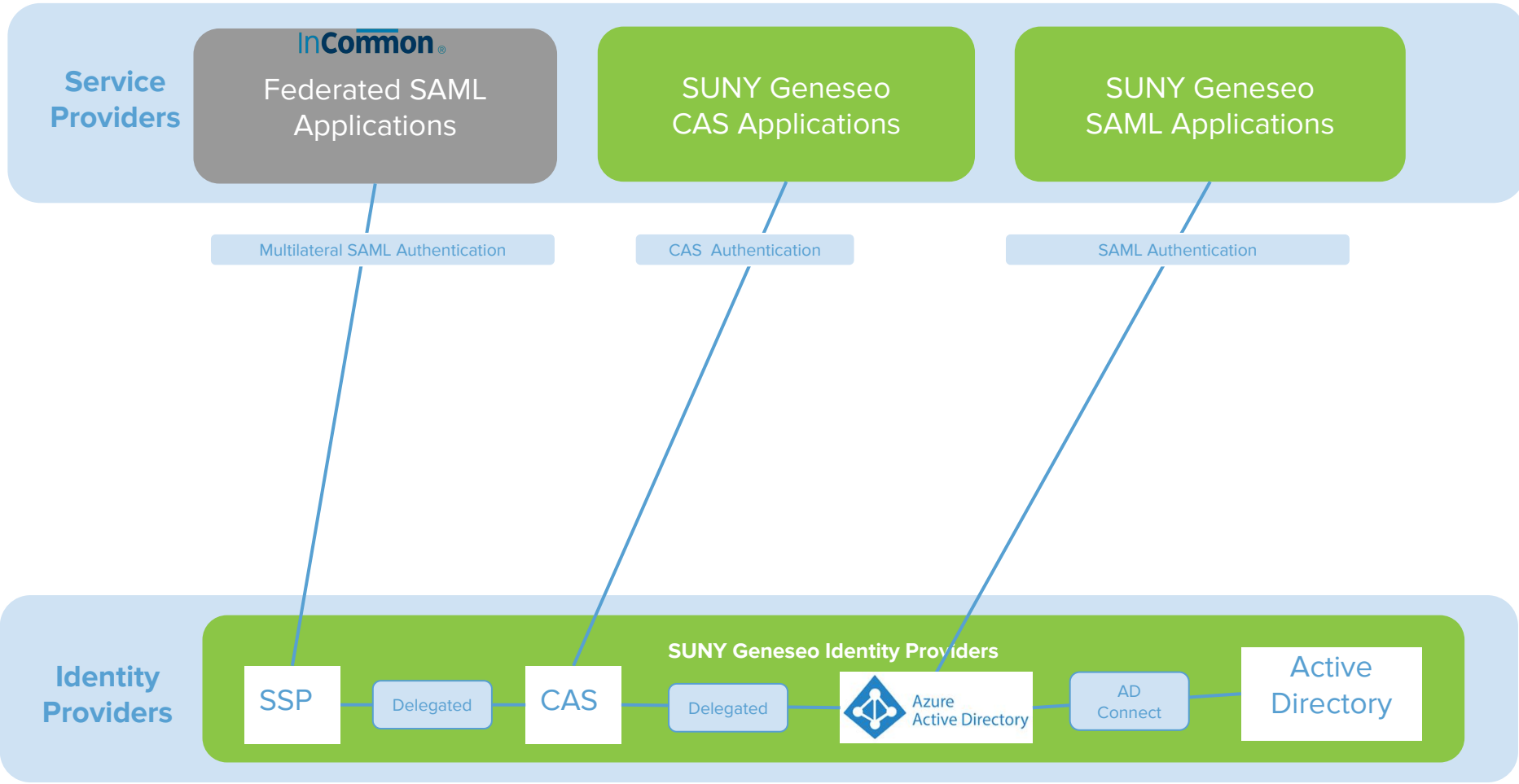


# SUNY Geneseo & Cirrus Implementation Overview

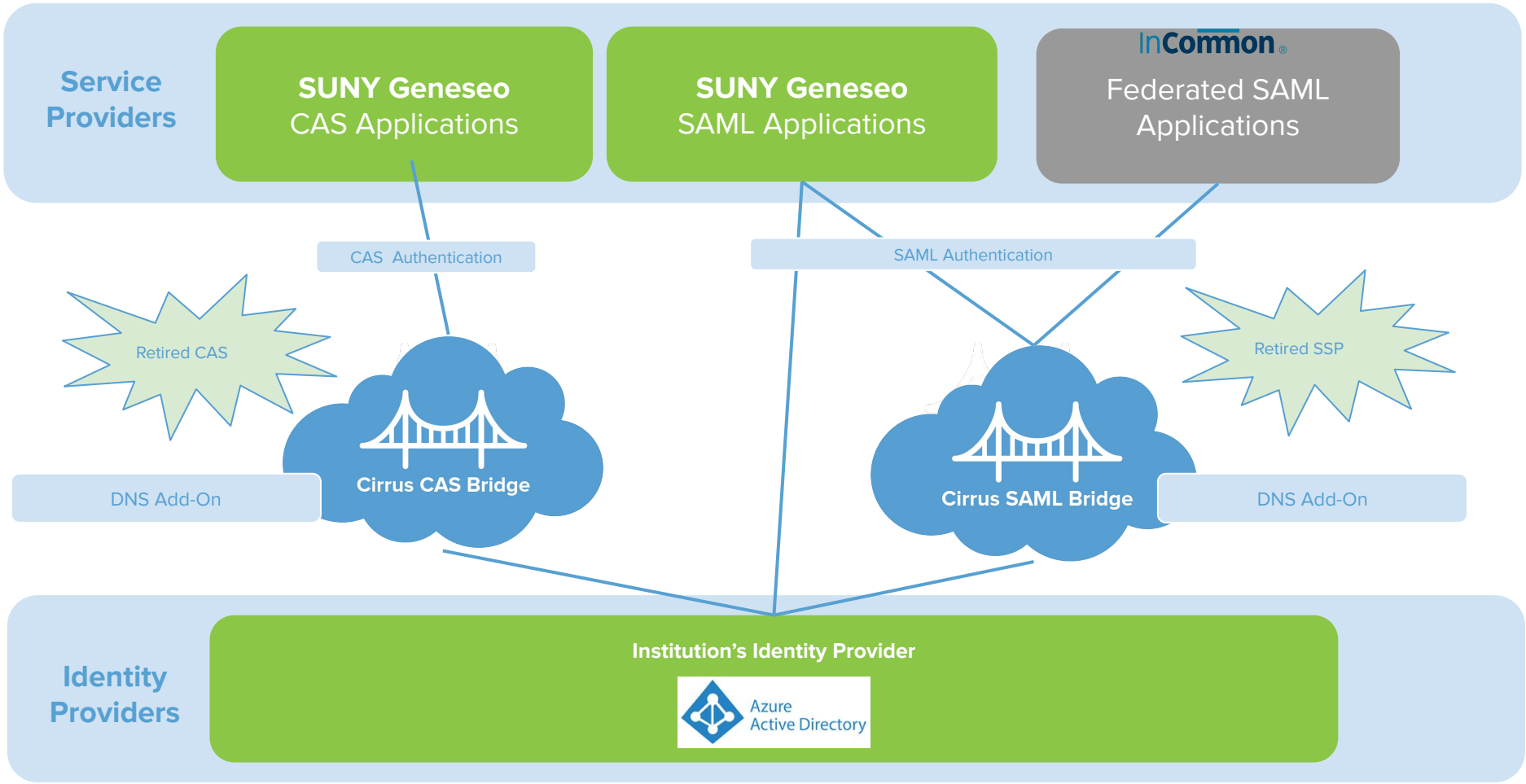


**GENESEO**  
THE STATE UNIVERSITY OF NEW YORK

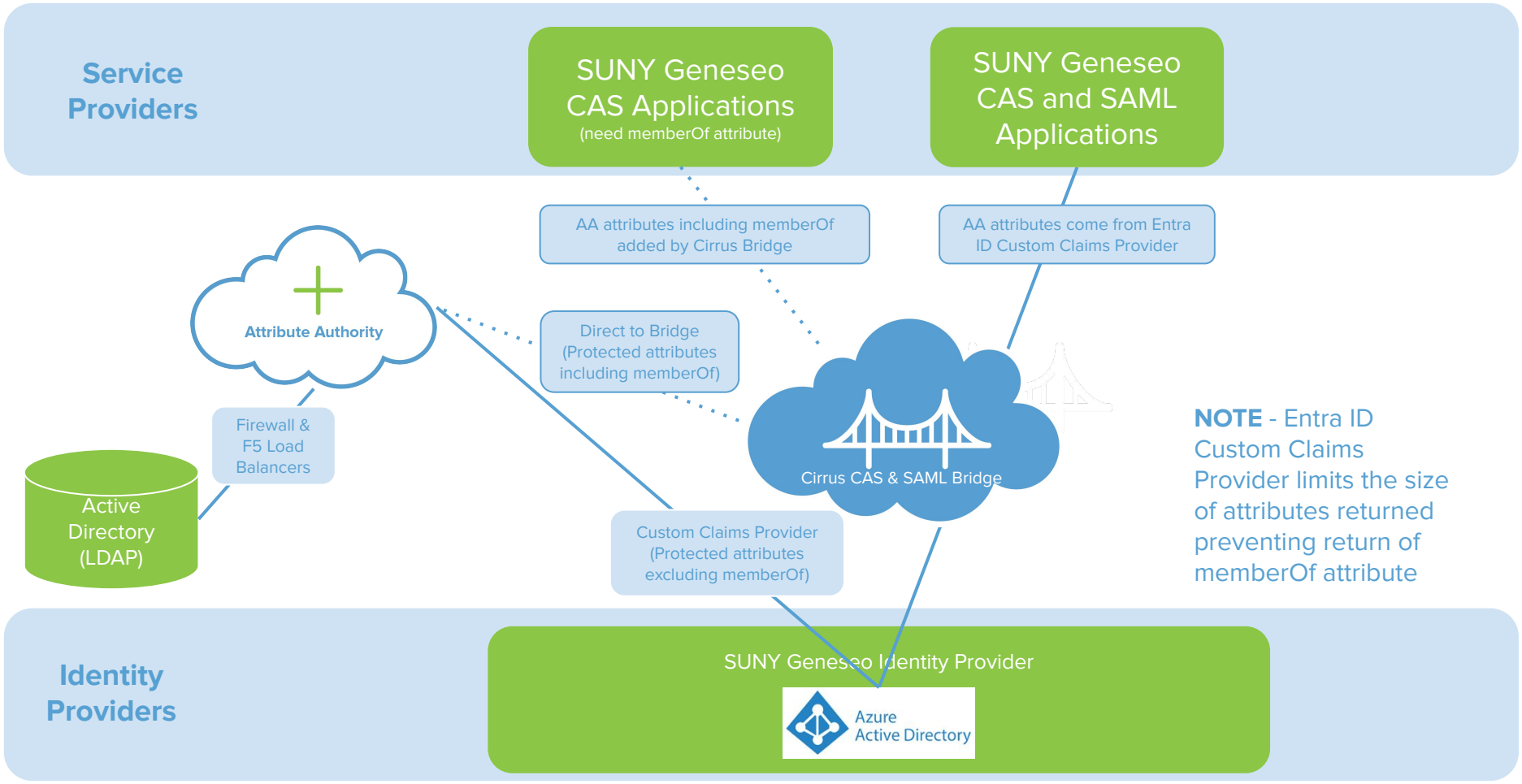
# SUNY Geneseo - Before Cirrus Bridge & Attribute Authority




# SUNY Geneseo - **After** Cirrus Bridge



# SUNY Geneseo - **After** Cirrus Attribute Authority



# SUNY Geneseo Login Screen - All Applications

 **GENESEO**  
THE STATE UNIVERSITY OF NEW YORK

## Sign in


Use your full email address

---

Can't access your account?

[Back](#) [Next](#)

By logging in you acknowledge and agree to the SUNY Geneseo Acceptable Use Policy. If you need help contact the CIT HelpDesk [help.geneseo.edu](http://help.geneseo.edu) or (585) 245-5588.

 [Sign-in options](#)

[Terms of use](#) [Privacy & cookies](#) ...





# SUNY Geneseo Advice & Lessons Learned



**GENESE0**  
THE STATE UNIVERSITY OF NEW YORK

# Advice & Lessons Learned:

- **Ounce of prevention / pound of cure (before Cirrus implementation)**
  - Aggressively migrated services to vanilla Azure AD that did not need Attribute Authority
  - ...which forced us to build an accurate inventory of services
  - ...which greatly simplified our Cirrus implementation
- **The attribute authority was very simple to implement from our end, and the configuration was well-documented by Cirrus.**
- **We suggest sharing your LDAP service peculiarities. We have load-balanced LDAPS (LDAP+SSL/TLS) service, and we believe it helped Cirrus to know our timeouts, for example.**
- **The DNS takeover feature is very nice.**
  - We had one misbehaving Java app that needed its OS DNS cache manually flushed
- **Cirrus Console is handy for troubleshooting “is the service hitting CAS validation endpoints?”**





# Questions?



**GENESEO**  
THE STATE UNIVERSITY OF NEW YORK

**Thank You!**

**Email [sales@cirrusidentity.com](mailto:sales@cirrusidentity.com)  
for more information**