Azure AD Federation - Gonzaga

The business pain point

Gonzaga had two goals:

- Access InCommon using Microsoft Azure AD
- Do it without running an on-prem solution

Gonzaga has invested in consolidating campus identity and access management to the Azure Active Directory platform. While this has served Gonzaga well, a gap existed.

Gonzaga, like any university of its size, has a research and scholarship mission. Access to services offered by the InCommon trust federation (https://incommon.org/) is necessary to support collaboration. Azure Active Directory's bilateral support for SAML integration doesn't provide the technical capability necessary to participate directly as an identity provider in InCommon.

How did Cirrus Identity help?

Gonzaga was looking for a solution that would bridge the gap between Azure AD and InCommon. They found it in the Cirrus Identity Bridge.

Depending on the license level of Azure AD; the way metadata is handled, SPs are registered, and attributes are released prevent registration as an InCommon Identity Provider. The Bridge addresses these issues by making the metadata available to InCommon and asserting attributes in the eduPerson schema expected by the federation service providers.

The Bridge is a hosted solution that saves customers the time and effort required to maintain an on-prem federation-friendly SAML Identity Provider. Cirrus Identity also brings many years of InCommon experience and SAML technical knowledge to help customers get their first integrations up and running quickly.


GONZAGA UNIVERSITY

Microsoft Azure

InCommon FEDERATION

Other SAML SPs
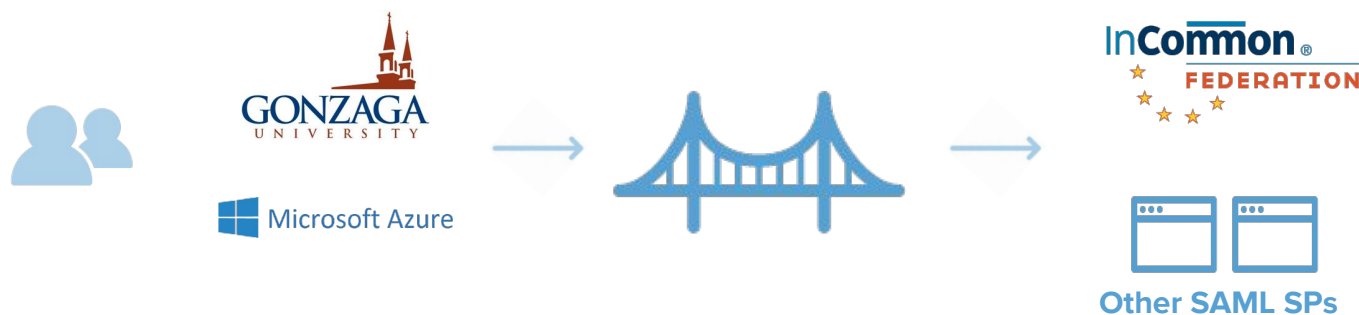
Azure AD Federation - Gonzaga

What do users see?

The key is end users do not see anything. An individual can start the day logging in for Office365. This initiates the Single Sign-On session in the user's browser, and as long as that session is active, the user can access other federated applications, including InCommon applications, without having to log in again.

The login screen is branded in Azure AD to match the organization's look and feel.
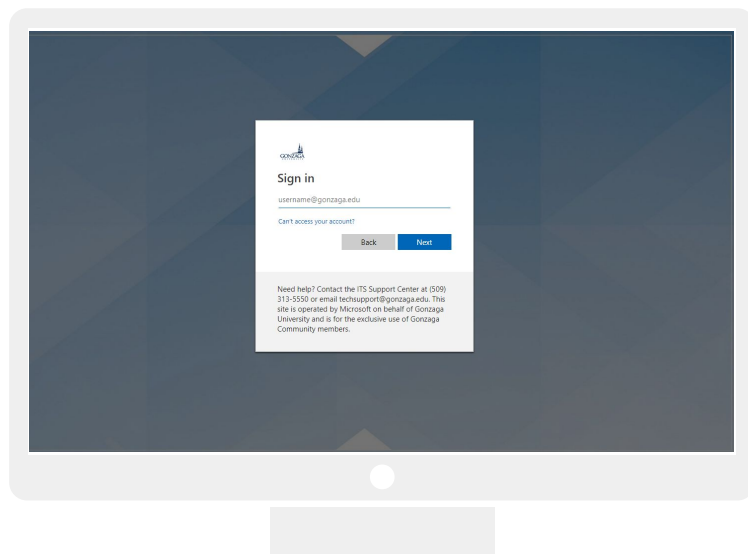
After initial login, a few minutes later, that same login provides seamless access for an InCommon federation application such as EDUCAUSE (pictured below) or any number of research and collaboration tools.

The only difference with InCommon-federated applications is the occasional need to choose the institution from a list when logging in. The dialog where the username and password are entered always remains the same.
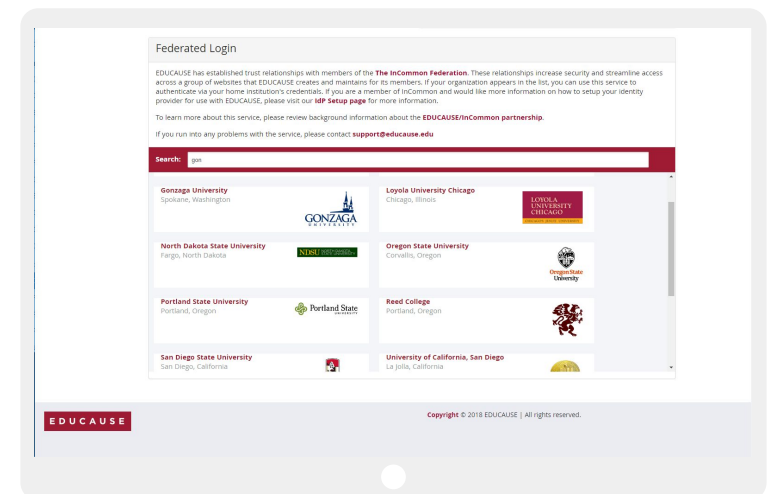
Azure AD Federation - Gonzaga

What do administrators see?

For the Azure AD administrator, there is a straightforward configuration in the Azure Portal to define a new web application. While the configuration depends on the license level, it requires only a few parameters provided by Cirrus Identity and less than 30 minutes.

After configuring the application, Gonzaga's InCommon admin was able to register the Cirrus Bridge as the organization's Identity Provider.

Cirrus Identity provides step-by-step documentation for the Azure AD configuration and InCommon registration.
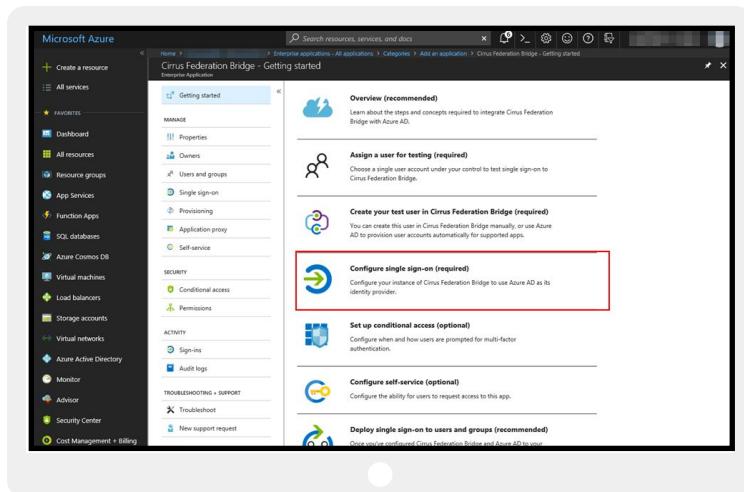
Implementation highlights

After InCommon published Gonzaga's IdP metadata, Gonzaga staff were able to demonstrate access just like any other InCommon member.

Gonzaga's premier licensing of Azure Active Directory enabled:

- Attribute release customization to add user attributes to the SAML assertion
- Access control for users allowed to access federation services using Active Directory groups
- Administrators use familiar Azure Portal tools to manage their InCommon participation

Azure AD Federation - Gonzaga

Cirrus Products Used

Bridge
A solution for when your existing IAM solution is not InCommon friendly or needs to support mesh style federation

Product Integrations

Microsoft
Azure Active Directory

InCommon®
FEDERATION

"We wanted to see the benefits of the InCommon Federation, and Cirrus Identity really helped us get there. Thanks to Cirrus, we are able to make federated identity management a cloud thing -- both technically and administratively. Cirrus provides a service that delivers the technology, a support team, and deep SAML knowledge so we can focus on other things. It's the ideal partnership"

- *Thomas Buck, Infrastructure Architect, Gonzaga University*