Okta and Cirrus Identity Bridge - CSUMB

The business pain point

CSU Monterey Bay (CSUMB) implemented Okta's IDM solutions to streamline integration of cloud services. A full migration to Okta was hampered by two gaps:

1. Okta's Identity Provider cannot readily integrate with Service Providers registered in the InCommon trust federation https://incommon.org/)
2. Some CSUMB enterprise apps require the CAS protocol which is not supported by Okta

Okta's SAML support is based on bilateral connections between Okta's identity store and each service provider. This architectural design makes Okta incompatible with mesh federations like InCommon that require a single IdP endpoint for an organization. With the deployment of Okta, CSUMB wanted to decommission their local Shibboleth deployment for InCommon participation.

Secondly, CSUMB relied on a CAS shim to support Single Sign-on to a few critical enterprise applications, including the course management system which saw large numbers of end users logging in every day. Okta does not provide a capability to integrate using the CAS protocol.

How did Cirrus Identity help?

The Bridge from Cirrus Identity addresses both the limitation of bilateral connections, and can be deployed with an add-on to support CAS protocol translation.

The Bridge securely consumes InCommon metadata, and supports the registration of a single SAML Identity Provider endpoint for participation in the federation. The Cirrus Bridge functions as an application within the Okta configuration, and Cirrus provides step-by-step instructions for setting up the Bridge within the Okta admin tools.

The Bridge can also be configured to assert attributes in the form expected by the federation.

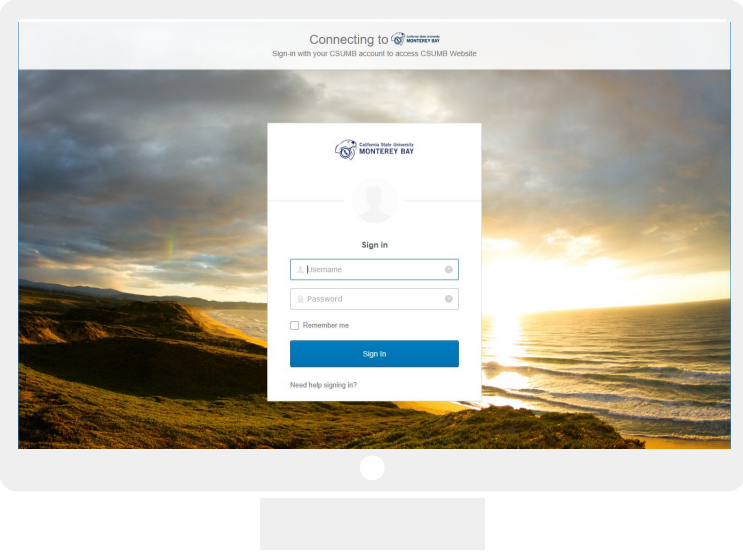
The CAS add-on translates assertions into the CAS protocol, and can also be configured to assert attributes in the format required by the CAS-enabled Service Providers.

The Bridge saves customers the time and effort they would need to maintain comparable solutions themselves. Cirrus Identity also brings many years of InCommon and CAS experience to help customers deploy to production quickly.

Okta and Cirrus Identity Bridge - CSUMB

What do users see?

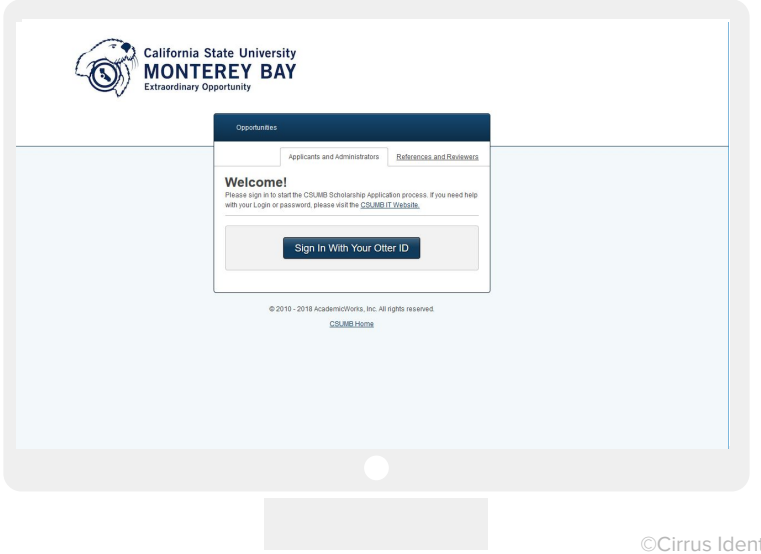
The key is end users do not see anything. An individual can start the day logging in for GSuite using Okta. Seamlessly, minutes later, that same login experience provides access for an InCommon federation application such as AcademicWorks used to manage scholarships (or the main CAS administrative systems). If the end user sees a login screen, it is always the same one.



The Administration Experience

For the Okta administrator, setup is a straightforward configuration in the Okta Portal to define a new application to point to the Cirrus Bridge. It requires only a few parameters provided by Cirrus Identity.

After the initial setup, service providers published in InCommon metadata are accessible provided sufficient attributes are released. Configuration of non-InCommon or CAS service providers, as well as configuration of attribute release is made by contacting Cirrus Support. In the future, these will be self-service capabilities in the Cirrus Console.



Okta and Cirrus Identity Bridge - CSUMB

Implementation highlights

The implementation started with an initial assessment of CSUMB's environment. This was used to build an initial deployment that could be tested by CSUMB staff.

During testing, it was identified that a dedicated Bridge was needed to support the network and security constraints of CSUMB's large CAS administrative applications. A dedicated CAS Bridge was deployed for those applications and a general purpose Bridge was deployed for InCommon and other CAS service providers.

The separate bridges also allowed the deployments to take place at separate times. The administrative Bridge was deployed first at a carefully scheduled deployment window coordinated with the associated applications. This allowed downtime to be minimized.

The separate deployments also enabled CSUMB administrators to apply separate policies within Okta. This allows each Bridge instance to have different user and MFA requirements.

Since CSUMB had already registered an IdP with InCommon, the certificates and DNS name were transferred to the general purpose Bridge. This enabled the change to be transparent to the InCommon federation.

The general purpose Bridge was deployed a few weeks after the administrative one (to accommodate CSUMB's schedule). As before, there was a deployment window to manage any disruption to the CSUMB community.

CSU Monterey Bay benefits:

- Retired local SAML IdP deployment
- Hosted solution freed up IT staff time
- Responsive support
- Stable operation
- Fills the gaps in their IDM strategy

Okta and Cirrus Identity Bridge - CSUMB

Cirrus Products Used

Bridge

A solution for when your existing IAM solution is not InCommon friendly, needs to support mesh style federation, or needs to go between the SAML and CAS protocols

Product Integrations

okta

InCommon FEDERATION

CAS

"At CSU Monterey Bay we have partnered with Cirrus, and have recieved top-notch support from them at every turn. I highly recommend them, Patrick is the best!

We are using their hosted environment to act as a SAML bridge between InCommon SAML SPs, CAS SPs, and our Okta IDM. It has worked perfectly."

- *Nick Rodrigues, Lead Network Operations Analyst, CSU Monterey Bay*