

The TIER Toolset: Campus Success for Lafayette College

As an investor campus, Lafayette College believes in the TIER vision. So, we were happy to be selected as one of the ten institutions chosen to participate in the Campus Success Program. In our proposal, we committed to integrating the TIER Shibboleth IdP package and evaluating the fourth TIER component, the midPoint identity registry.

The three TIER components were already a key part of our identity management system. Lafayette joined the InCommon Federation in 2007 and we were an early adopter of Shibboleth, running a local Identity Provider at our small liberal arts college. Recently, we became heavy users of Grouper and worked with Spherical Cow Group to add features to COmanage to support our use case for provisioning accounts and identity lifecycle management for affiliates of the College. Still, this all didn't mean there were no operational gaps needing to be addressed.

Moving to a containerized version of the IdP seemed like an easy decision for us. We aren't yet using Docker at Lafayette so there is a learning curve there and we need to work out the environmental requirements. The benefits we see in the TIER package are ease of deployment to new nodes and a default configuration geared towards doing things the InCommon Way: an interoperable IdP that releases a default set of attributes and supports MFA.

Being able to investigate how the midPoint entity registry works really piqued our interest. Our system of record for faculty, staff, and students is Banner. We have a custom-engineered IdMS for faculty and staff onboarding. It's a mix of web forms, a database, and Perl scripts that provision accounts to our LDAP directory. Provisioning of students we do using extracts from Banner and scripts. So, the process is manual. The goal of hooking up midPoint to Banner to get the identity data to flow will be finally doing near real-time provisioning from our ERP. That's been a long time coming. We're also looking at creating and assigning our digital identifier, the Lafayette NetID, using midPoint. We'll see if midPoint has a capability that can do that.