Putting **access management** at the foundation of **student success** at San Jose State University

By EdScoop Staff

A university campus can often be a chaotic, disjointed environment for IT support professionals. At San Jose State University, part of the California State University system, the IT staff have implemented a new identity and access management platform that not only helps bring some order to their environment, but also supports a more fundamental goal – promoting student success.

Implementing a system that allows students to access all of their applications and student information systems through a single access point, using a single password, might seem like a logical investment. But the SJSU IT support staff have seen a cascading effect of operational improvements, starting with a major reduction in help desk calls, which frees up personnel to take on more complex assignments.

Just as important, it is making students' online activities easier and less frustrating, which advances a key goal of the larger California university system.

"CSU has a system that's very focused on improving graduation rates," said Michael Cook, SJSU's Director of Customer Service and Information Security. "Students are taking five to five and a half years [to graduate], so we're very focused on getting them down to the four years it should be … Anything we can do to make their lives smoother and easier helps their success rate on campus."

SJSU is the oldest, and one of the largest, universities in the California higher education system, with more than 32,000 students and another 5,000 or so faculty and staff. Meeting their IT needs has resulted in managing "in excess of 100 web-based applications," Cook said. Many of those applications tie into proprietary systems with unique sign-on requirements.

"There were so many different applications, so many different passwords, students were just throwing their hands up, sharing passwords, writing them on sticky notes and leaving them out," he said. "It was challenging for us to support multiple identification systems. Someone would call the help desk and first we'd have to figure out what system it was, then find someone on our staff able to support that."

Joel Johnson, IT Director for Web and Campus Applications at SJSU, said that a growing challenge led the department in search of a solution that could support a lot of different applications, be transparent to users and integrate with SJSU's existing system of record for identity management. And it had to be easy to manage, configure and support.

They also wanted a solution that would reduce the number of questions to the help desk and allow support staff to know where users are in the authentication process. "And we wanted a large player in the identity space, so they would be adding enhancements and new capabilities regularly," Johnson said. "Cost is always a factor in any purchase the university makes, but it was probably secondary to those."

After evaluating potential solutions, Johnson and Cook selected the Okta Identity Cloud.

"We are using the core API products, which include single sign-on and Universal Directory," Johnson said. His team started the implementation with a small number of applications initially, bridging them to an existing PeopleSoft system, which assigns users to groups for application access. It helped that Okta's products are compatible with PeopleSoft.

The big step was when SJSU integrated Okta with Shibboleth, the university's existing single sign-on product, which is proprietary and requires extensive training. It went seamlessly. "We let applications think they're authenticating with Shibboleth, but it just does an authentication relay to Okta; Okta then tells Shibboleth it's OK to grant access," Johnson said.

Now, when a prospective student, for instance, goes through the SJSU application process, they get provisioned online as an applicant. If they're accepted and decide to attend, as soon as they register for a class, the student's group designation switches from applicant to student status and they're automatically authorized for all student apps. Each time their status changes – for instance, they become a student assistant, or they get a campus job – Okta automatically handles the access credentials of the groups they're in and the apps they can use.

The university's various departments all have wholeheartedly supported the change, Johnson said. "They don't have to worry about how authorization works, how people are signing in [or] creating new accounts," he said. And configuring new applications into Okta takes just minutes, as long as they support the Security Assertion Markup Language (SAML) standard. Setting up the students for single sign-on went so smoothly, the staff also rolled these solutions out internally for faculty and staff.

"We no longer have any serious concerns around people misusing or trying to work around security practices or sharing accounts or passwords," Cook said. "The environment is so simple we don't get any pushback or concerns around misuse ... and we can monitor and implement security measures pretty easily."

Their advice to other colleges and universities considering improving their sign-on processes? Go for it.

"I'd say trust this solution; trust it'll work, and the sooner the better – it'll make your life easier," Cook said.

"Be more aggressive than you perhaps thought you could about getting to single sign-on," Johnson suggested. "Be pretty aggressive, because it's easy to move, easy to configure, and you'll get to the end state of single sign-on pretty quickly."

This article was produced by EdScoop for, and sponsored by, Okta.