Case Study
Indiana Institute of Technology

About Indiana Tech

Indiana Tech, a prestigious Fort Wayne university founded in 1930, serves 8,000 active students and 1,500 faculty. The institution relies on PortalGuard for Enterprise-ready support and deployment, alongside Self-Service Password Reset and Single Sign-On to various Education-related web apps.

The Challenge

Indiana Tech was finding that its security software, ADFS, was not up to par, with its lack of a brandable login form, no support for the CAS SSO protocol, and the inability for ADFS to distinguish between staff and students. ADFS required multiple servers, weighing down the university's infrastructure. The lack of a web application for their Help Desk worsened these problems, and the situation always escalated right at the beginning of new semesters, when numerous students would forget and/or have to change their passwords – bumping up hard against ADFS's lack of a self-service password reset feature. As a result, engineers became overwhelmed, and user downtime was a huge problem.

The PortalGuard Solution

Indiana Tech, due to their high traffic, needed something smoother, better, and more seamless. They needed a product that anticipated the surge in forgotten passwords that occurs at the start of every semester, and allowed an automated, secure solution for self-service, so engineers would no longer be flooded with requests. They also required different security policies for staff, students, and so on. Essentially, Indiana Tech needed a product that was customizable, intuitive, less rigid, and efficient.

That's why Indiana Tech turned to PortalGuard, which provided the solution they were looking for.

Customer Profile

Industry:

Higher Education

9,500+ Users

Location:

Indiana

Top Applications Used:

AD, Office 365, Blackboard and Jenzabar

The Results

PortalGuard recognized Indiana Tech's every need and got to work meeting each requirement. Distinguishing between staff and students was easy: By using PortalGuard, Indiana Tech now boasts six separate security policies – students, faculty, adjunct, staff, IT, and admins – with different features available to each.

Thanks to PortalGuard, Indiana Tech now has automated self-service password software, currently handling an average of 500 password resets a month, allowing users to unlock their accounts using questions and/or the user's cell phone, and sending automatic password expiration reminder emails 14 days in advance. Because of these changes, the beginnings of new semesters are no longer hectic for the engineers. Meanwhile, PortalGuard's software is highly flexible, incredibly customizable, and offers multiple languages. It provides security where needed, constant stability, and by requiring only one server in a hosted data center, eats up fewer resources. The seamless integration of Duo, a cloud-based two-factor authentication service, and PortalGuard immensely reduces help desk calls.

Furthermore, any time Indiana Tech needs a hand, PortalGuard is there, and dedicated to providing outstanding support at every turn. Effective, integrative, and easy-to-use – that's the PortalGuard promise.

An Enterprise Ready Solution

The PortalGuard Enterprise solution was created as a RESTful web application, which allows it to scale out horizontally for performance and load balancing by adding additional servers as needed. Each application server has a suggested threshold of 10,000 concurrent users - with properly configured load balancing, Indiana Tech was easily able to meet the traffic and uptime necessary for their 9,500+ user base.

Additional Resources

Why Indiana Tech Chose PortalGuard vs. AD FS

SAML Single Sign On Tech Brief

Centralized Self-Service Password Reset Tech Brief

Overcoming 2FA Hurdles Tech Brief

PortalGuard is a cybersecurity authentication package that delivers a full set of features in a single, fully customizable solution. PortalGuard provides single sign-on (SSO), self-service password reset (SSPR), two-factor authentication (2FA), and over 130 other features to ensure that each campus is equipped with the tools needed to face any authentication challenge.