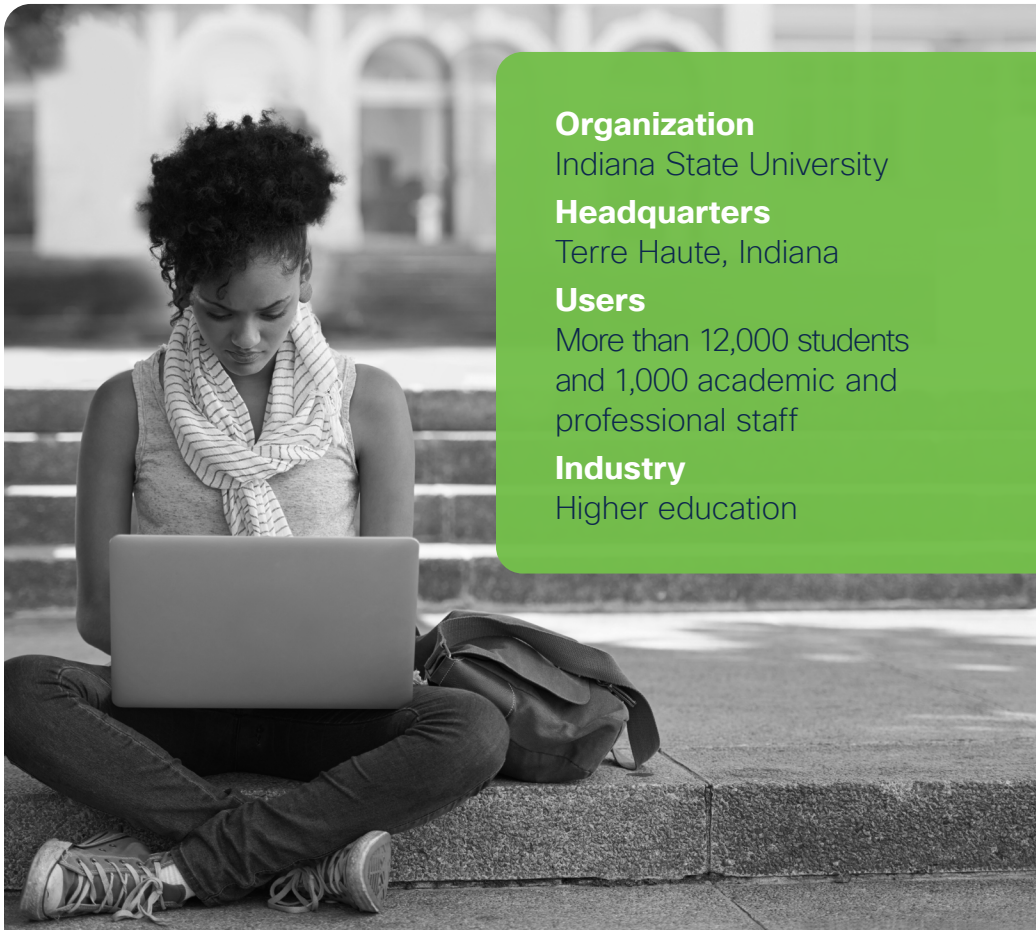
# How a university provides seamless network access from anywhere while maintaining a strong security posture

Established in 1865, Indiana State University ranks among the best colleges in the United States for its innovation and educational programs. With more than 100 under-graduate and 75 graduate programs offered, the 700 academic staff and 300 professional staff serve more than 12,000 enrolled students. Supporting business objectives while reducing risks is a constant balancing act for the university's three-person network team.



**Organization**
Indiana State University

**Headquarters**
Terre Haute, Indiana

**Users**
More than 12,000 students and 1,000 academic and professional staff

**Industry**
Higher education

## Objective

In a higher education environment, supporting academic freedom and open access while protecting the network from threats requires a delicate balance. For Indiana State University, this meant maintaining visibility into 50,000 endpoints connecting to the network each month, including 40,000 unmanaged devices. The university wanted not only more comprehensive controls but also a simple and seamless experience for its diverse user base.



## Solutions

- Cisco Identity Services Engine
- Cisco Platform Exchange Grid
- Cisco Secure Firewall

## Impact

- Gained dynamic visibility into devices connecting to the network, along with detailed, role-based controls.
- Streamlined access control and policy management while simplifying compliance and auditing.
- Segmented the network while providing guest and secure wireless access.
- Boosted security posture with automated threat containment.
- Improved student service with a simple, seamless user experience.

## Providing the right level of access to the right people and devices

"The big problem in an academic environment is that we have to support academic freedom and freely give away the connection and, at the same time, we're trying to maintain security and the knowledge of who's on our network," explains David Pifer, Indiana State University's assistant director of network engineering services. "One set of people would just assume that it's all turned on, anybody can use it, and we never want to know who the users are. And the other side of it is that if something goes wrong, we need to figure out what happened."

Maintaining this balance is especially a challenge when in any given month, more than 50,000 endpoints connect to the network. Those connections include not only student and staff devices but also campus visitors with guest access. The university owns or controls only about 10,000 of the devices accessing resources. "In an academic environment, we have an inverted BYOD model compared to most corporations," Pifer says.

To improve security posture while serving the needs of diverse users, Indiana State needed a solution that provides dynamic visibility into the endpoints connecting to the network, automates threat containment, segments the network, and enables guest and secure wireless access. The network team also wanted to offer a simple, streamlined user experience, both for the campus community and for guests.

> "In an academic environment, we have an inverted BYOD model compared to most corporations"
>
> David Pifer
> Assistant Director of Network Engineering Services, Indiana State University

## Supporting the needs of diverse users while maintaining strong security posture

Indiana State University deployed Cisco Identity Services Engine (ISE) for network access control for the wired and wireless environments. With ISE, Pifer's team can identify and authenticate users, provide the right access levels, and track who's on the network and if their activities are causing problems for other network users. "ISE streamlines policy management and makes it very easy to look at different aspects of a user, the workstation, the environment, or the way they're connecting into our network," Pifer says. "And it helps us assign them the appropriate role very quickly."

With ISE providing visibility and control, Indiana State reached a point where "everything is pretty secure and we really don't get that deep into the weeds on chasing down issues unless it's a significant event," Pifer notes. "We've got a good posture established, and users are happy because they can connect in. We're able to set up guest registration, so when people come in, they can self-register on our campus and use our wireless. We're leveraging this tool to give them some freedom."

ISE also serves as the university's authentication component for the Cisco AnyConnect VPN through Cisco Secure Firewall (Firepower). Integration with Firepower and Cisco Platform Exchange Grid (pxGrid) provides further value by enabling the network team to isolate or restrict network access to individual devices or entire groups suspected of compromise.

The comprehensive set of capabilities—including visibility, role-based policy controls, and automated threat containment—made ISE instrumental to maintaining business continuity during the COVID-19 pandemic, enabling a fast, smooth conversion to a remote learning environment with minimal impact to users. "ISE was really critical because it helped provide seamless transition as users moved from on-campus to off-campus use," Pifer says. "Everything worked well and users didn't really have that many issues."

That experience created a mindset shift toward a long-lasting remote environment, and ISE removed the concern about whether remote access can be achieved securely and easily. "Coming out of this, I think we are prepared to provide a more secure and reliable environment when our users need to work, learn, or teach remotely, and ISE will be instrumental to supporting that need," Pifer says.

> "ISE streamlines policy management and makes it very easy to look at different aspects of a user, the workstation, the environment, or the way they're connecting into our network. And it helps us assign them the appropriate role very quickly."
>
> David Pifer
> Assistant Director of Network Engineering Services, Indiana State University

## Seamless, streamlined experience for staff, faculty, and students—regardless of where they connect

The top outcomes of the ISE implementation for the university were device segmentation and identification of who or what is on the network, according to Pifer. "We're able to see a user and where that person is connected to our network. If there's a problem, we know who to talk to because it's not just a random device causing an issue. We can figure out what the problem is and resolve it," he said.

These capabilities not only improve security but also provide an asset inventory and simplify compliance and auditing. "We've got a fairly good idea of who or what is on our network with ISE," Pifer explains. "It gives us a little bit of a fingerprint of people, a better pulse of what type of devices we're having so we can tailor our network around what the end users are bringing on our campus."

The most valuable outcome was improved service to the students, who expect and demand instant access. Pifer recalls past struggles to onboard users. At the beginning of every semester, as many as 500 students would line up at a walk-in help center for assistance with access. Now, onboarding is fast and students have frictionless experience, regardless of where they connect. "ISE has simplified our users' experience and decomplicated the process to log in to the network," Pifer says. "Our students can move anywhere around campus and ISE just lets them back in. It's really seamless to the end user."

As Indiana State embarks on a journey to zero-trust security, the network team plans to use ISE to further boost security by continually verifying endpoint trust; enforcing policies based on least privilege; and connecting students, staff, and visitors to trusted resources.

"ISE will be the piece that gathers the information and decides if this is a computer or user we trust, and where they are located. And it'll feed the information back to either the wireless controller or the switch to tell it how to handle that user," Pifer says. "We've always aspired to the idea of zero trust, and I see ISE being a critical part of that process."

To learn more visit: cisco.com/go/ise and to watch a demo on ISE click here.