

School District Simplifies Building Access Control



Judson Independent School District implemented centralized physical access control system.

EXECUTIVE SUMMARY

JUDSON INDEPENDENT SCHOOL DISTRICT

- Education
- San Antonio, Texas
- 22,000 Students; 3000 Employees

CHALLENGE

- Create safer campuses
- Simplify management of physical access control
- Reduce upfront and ongoing costs

SOLUTION

- Cisco Physical Access Control, enabling centralized scheduling and management of exterior doors for different campuses
- Integration with Microsoft Active Directory, eliminating manual entry of employee information

RESULTS

- Accelerated adding and deleting door access privileges
- Saved 80 percent on deployment costs
- Freed up IT staff time

Challenge

Located in northeast San Antonio, Texas, Judson Independent School District (JISD) is the city's fourth largest district, with 27 schools, 22,000 students, and several thousand employees. Population growth has transformed JISD from a small-town district into more of an urban district, with a greater need for centralized physical security measures such as automated locking of exterior doors.

When the IT department saw the contractor's plans for a new building with a traditional physical access control, the department decided to look for a centralized solution instead. "To reduce costs and improve controls, the district is centralizing all of its information technology," says Steve Young, chief technology officer for JISD. For example, application servers now reside in an administration building instead of on individual campuses, and teachers and staff access the applications over the Cisco network.

With the solution the contractor proposed, each location would need an expensive central panel, in addition to a smaller panel for each door.

This is not a cost-effective design for the district, because many buildings only require access controls for one or two doors. In addition, every time an employee joined or left the district, the IT team would have to manually add or remove that person from the database.

Chief requirements for the new physical access control solution were simplicity, ease of user management, and low cost. “Along with 21st century learning, physical safety and administrative efficiency are top priorities for the district,” Young says. “The physical access control system contributes to both goals.”

Solution

After a yearlong evaluation, JISD selected the Cisco® Physical Access Control solution. “Unlike physical access control solutions from door and camera vendors, the Cisco solution takes full advantage of IP network capabilities, such as integration with Microsoft Active Directory,” Young says. The ability to integrate the Cisco Physical Access Control solution with Active Directory would eliminate the tedious chore of manually adding or deleting employee records whenever an employee joined or left the district. The IT team also liked the centralized architecture, because individual campuses would not need their own central door controller, for significant cost savings.

JISD installed two Cisco Physical Access Manager servers in one building, for resilience. The door hardware and proximity-style badge readers connect to the centralized servers through a Cisco Physical Access Gateway. So far, JISD has added six schools with a total of 19 doors.

The IT department uses an intuitive web-based interface to assign different privileges to different groups of employees. For example, principals and head custodians have 24-hour access to all areas, while teachers and aides have limited access. The same interface is used to schedule when various doors are locked. JISD automatically locks and unlocks certain doors. Other doors remain locked all the time but will open for employees with badges during certain hours, such as 6:30 a.m. to 5:00 p.m. on school days.

“To add physical access control in other buildings, we only need to purchase the door gateways that connect the door hardware and badge readers to the network, not to an expensive control panel.”

—Steve Young, Chief Technology Officer, Judson Independent School District

Results

Safer Campus

The Cisco Physical Access solution contributes to campus safety in multiple ways:

- **Automated door locking and unlocking:** “Knowing that exterior doors will be locked at the appropriate times gives principals peace of mind,” Young says.
- **Building access reports:** The system produces logs showing when people used their badges to enter buildings. If an incident occurs, security personnel can look at surveillance video corresponding to the time of entry to see activities leading up to an incident.
- **Ability to quickly disable badges:** If the district terminates an employee, that employee’s building access is terminated as soon as the new status is entered into Active Directory. The IT or security team does not need to separately remove the employee from the Cisco Physical Access Control system, a source of delays and increased security risk.
- **Remote management, for emergencies:** Authorized staff can activate or deactivate access accounts from anywhere, using any desktop or laptop with web access.
- **Fast lockdowns:** For one campus, the IT team has created a link that authorized users can click to lock down all exterior doors at once.

“Knowing that exterior doors will be locked at the appropriate times gives principals peace of mind.”

—Steve Young, Chief Technology Officer, Judson Independent School District

Cost Savings

Implementing Cisco Physical Access Control solution cost 80 percent less than the other architectures that the district evaluated. “To add physical access control in other buildings, we only need to purchase the door gateways that connect the door hardware and badge readers to the network, not an expensive control panel,” Young says.

The architecture also makes it cost-effective to add one door at a time, something the district did recently for a newly built middle school wing. With other architectures, adding just one or two doors is not financially feasible because each building requires its own control panel.

Still more cost savings come from not having to reissue lost keys and change locks if the lost key poses a security risk. “Our principals are very pleased to be getting out of the key business, which is a nightmare for schools,” Young says.



Staff Time Savings

The IT team now spends less time adding new employees. “We can assign building access privileges about twice as fast as before,” Young says. “We probably save a couple of hours every month.” The reason is that staff can use employee information already entered into Active Directory instead of separately entering the information, a time-consuming and error-prone process.

IT staff also appreciate being able to make changes in access privileges from any location, even home. “We receive calls after hours, and appreciate not having to drive to campus,” Young says. The district did not have to train employees to manage a new network, because Cisco Physical Access Control solution resides on the same network the district already uses for learning applications, business applications, and Cisco Unified Communications Manager.

Flexibility to Meet Evolving Needs

Finally, the district has the flexibility to adapt the physical access control system for different needs, increasing return on investment. People who need entry to a loading dock, for example, use an IP-connected intercom to request entry, and then a staff member at the other side of the building can press a button to open the door remotely. Similarly, in an alarmed warehouse used for electronics equipment, JISD came up with an innovative way to integrate the Cisco Physical Access Control with the alarm system. Instead of entering a code to deactivate the alarm, people simply use their badges. This arrangement has reduced false alarms resulting from people forgetting the deactivation code.

PRODUCT LIST

Physical Security

- Cisco Physical Access Control

Next Steps

The district will add more buildings to the system, and gradually replace existing systems with Cisco Physical Access Gateways.

Certain sites might begin using biometric readers in place of badge

readers. Another possibility is to use the badge readers for time and attendance, further increasing the return on investment.

For More Information

To learn more about Cisco Physical Security Systems, visit: <http://www.cisco.com/go/physicalsecurity>.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (10020)