

Case Study

Adani Institute of Infrastructure Management
– AIIM (Ahmedabad, Gujarat)

Access Control Management System



- ◆ 95 Doors
- ◆ 9 Controllers Positioned
- ◆ 96 Access Control Readers Installed
- ◆ 1 Site Utilizing Mantra's ACS Application

System Overview

An access control system is a system which enables an authority to control the access of people to a building or certain areas. The system identifies, authenticates and authorizes entry of a person into the premises thereby giving complete protection and granting flexible control over who is allowed to enter the environment or a facility.

The access control system is one of the most commonly used systems in electronic door control using a card or a magnetic stripe and/or biometric devices which can be accessed by swiping through a reader on the door.

The general operations in access control include presenting credentials to the reader which further sends the credentials to the control panel (a highly reliable processor). The control panel then compares the credentials with an access control list (ACL) to verify/authenticate an individual for granting/denying the presented request. It then sends the transaction log to the database. If the access is denied based on ACL, then the door remains locked. If there is a match between the credential and ACL, then the control panel operates a relay that in turn unlocks the door. Often the reader provides feedback, such as flashing red LED for an access denied and green LED for an access granted.

About Client

Established in 2009, an infrastructure management educational institute - Adani Institute of Infrastructure Management (AIIM) is located within a sprawling 600-acres area of Adani Shantigram, the largest integrated township in Gujarat. AIIM has been at the forefront of infrastructure management education in a scientific and specialized manner, with its synthesis of research, consulting and education. AIIM campus provides learning ambience for intellectual excitement, fruitful interaction and professional growth. The campus comprises of spacious libraries, labs, workshops, indoor sports facilities, tutorial rooms and spacious canteen within the premises. For any educational institute spread over a vast land it is imperative to keep a track of students, teachers and staff entering or leaving the campus premises, restricting unauthorized entry on the campus and safeguard the people within the premises.

Challenges

One of the greatest challenges for any education establishment is balancing the need to create an open, stimulating and secure environment, while ensuring that people and equipment are protected from the threat of theft, vandalism and physical attack. In order to safeguard the campus of the university, increase the security and satisfy the need to minimize the complexity of managing access, AIIM decided to implement highly secure and reliable access control solution.

The Solution

To help AIIM in maintaining and overseeing the entry/exit of an individual within the premises of the university and control the access of students, staff and educators to certain areas, Mantra Softech provided them with an ideal access control system – a combination of both hardware and software.

1. Access Control Hardware

Mantra's access control hardware consists of various components which are positioned at different access control points on the campus. An access control point can be a door or other physical barriers where granting access can be electronically controlled. An electronic access control door can contain several elements. At its most basic there is an electronic lock and to automate this we place card reader. At AIIM only entry is controlled with the help of card readers and exit is done by push button switch.

The access control decisions are made by comparing the credential to an access control list. This lookup is done on the control panel. The communication between access control reader and controller is with the RS485 network, which is most common and widely acceptable communication technology for the access control solutions. Following hardware components have been deployed at AIIMS' facility:

1.1 Controller / Control Panel:

The access control permissions are processed and granted by the controller based on the available access list at the controller. Multiple controllers communicate with central access control software deployed at central server computer via RJ45 network. Controller gets the card number from various readers and it compares the same ID from the access list available in controller. The controller only sends an event to relay and based on an access list, an event can be accepted or denied.



- 1.2 Power Supply:
A centralized power supply unit has been placed to give proper DC power to all the controllers / readers / relays and locks.
- 1.3 Mifare Reader:
Reader only read card unique serial number and send the information to control panel. It also flashing LED or sound buzzer based on signal received by controller.
- 1.4 Relay Junction:
This device gets the signal from the controller and according to the signal; it switches the relay to operate the lock. This really has some self intelligence so it can automatically unlock the door during emergencies.
- 1.5 Electric Strike: An electric strike is an access control device used for doors and is intended for door security. It provides remote electrical control to unlock a door. It generally comes with two configurations like fail safe and fail secure. The fail-safe configuration locks the door when the electric current is applied to the strike. With the fail-secure configuration the door is locked until an electric current is applied to unlock the door.
- 1.6 Bolt Lock: The bolt lock is a locking mechanism distinct from a spring bolt lock because a deadbolt cannot be moved to open position except by rotating the lock cylinder. The common bolt uses a spring to hold a bolt in place, allowing retraction by applying force to the bolt itself. A deadbolt can, therefore, make a door more resistant to entry without a valid card.
- 1.7 Magnetic Lock: The magnetic lock is a simple locking device that consists of an electromagnet and armature plate. The electromagnet portion of the lock is attached to the door frame and a mating armature plate is attached to the door.
- 1.8 Double Magnetic Lock: It has the same functionality of the magnetic lock with an additional feature of being mounted on double sized door.

2. Access Control Software

Mantra's access control software is a centralized access control application, which provides an upload access control list to the control panel. It also maintains access control permission based on user rights as well as authorized and unauthorized access permission. Mantra's access control software can show all the log transactions made at access control readers in the appropriate reporting format. ACS application collects data from various access control readers or doors and sends it to the central database at AIIM. Then it uploads an access control rights list to the controllers.

Application Login screen

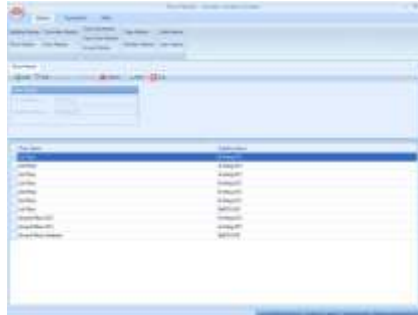


Application Master Menu

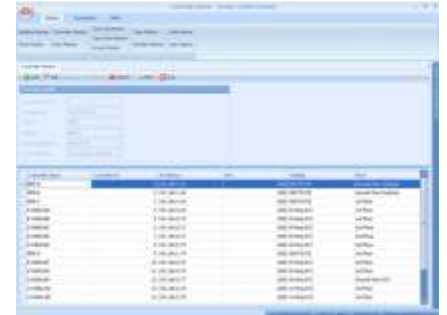
Building Master



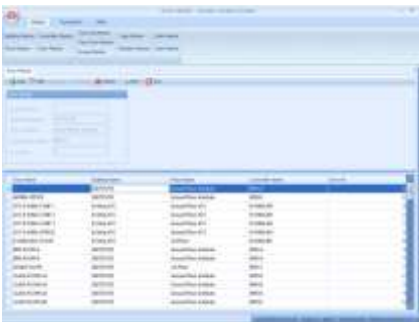
Floor Master



Controller Master



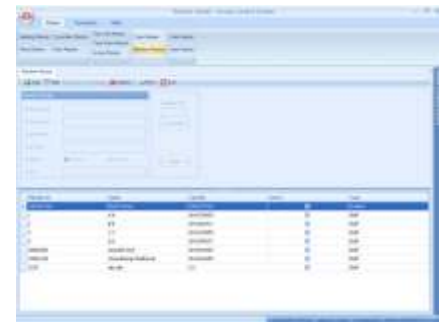
Door Master



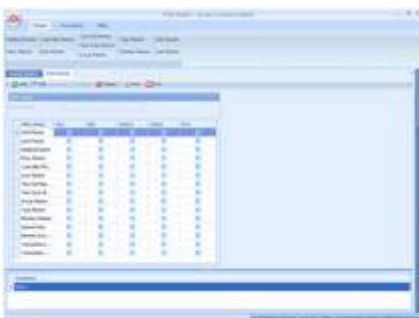
Time Set Master



Member Master



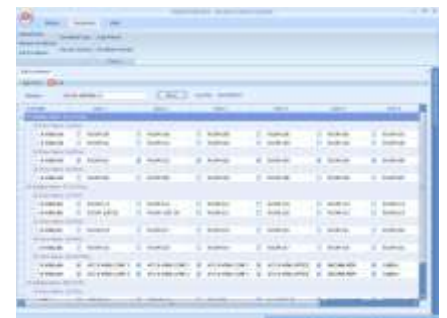
Role Master/User Master



Transaction Menu



Edit Enrollment



Benefits of Electronic and Card-Based Access Control System

1. Difficult to Duplicate

While physical keys can be copied very easily, duplicating electronic keys requires a much higher degree of sophistication. This makes your access system much more secure than it could ever be with physical keys.

2. Never have to change the locks

An electronic user database means that you never have to change locks at your premises or facilities. If a key card is ever lost, it can be removed from the database and a new one can be issued. If a person is no longer associated with the organization, site or campus, then his or her access rights can be deleted within seconds. This greatly lowers your overall exposure to risk.

3. Monitoring Reports

When someone tries to use a key in a lock and fails, you can never tell that the event happened, unless you catch them in the act. Someone can use a stolen key on several occasions, until the time is right or to get into a forbidden company area, thus causing damage more than once.

Since electronic access control systems record each transaction, you can keep an audit trail of all access attempts, and print out reports for specific areas, times and dates.