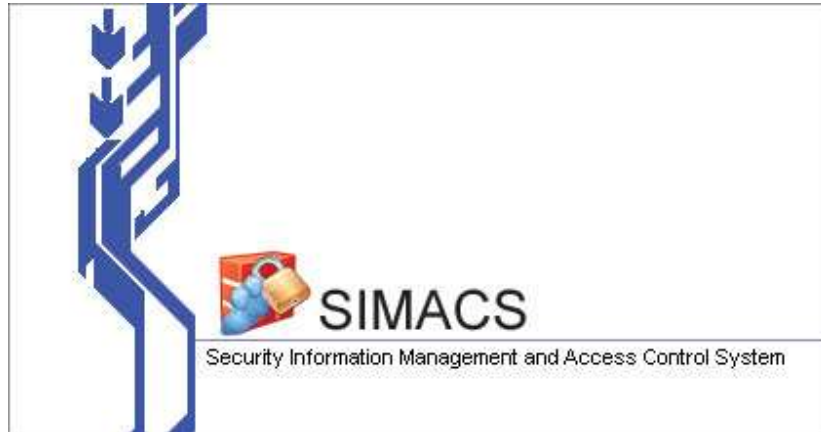


Security Information Management and Access Control System (SIMACS)



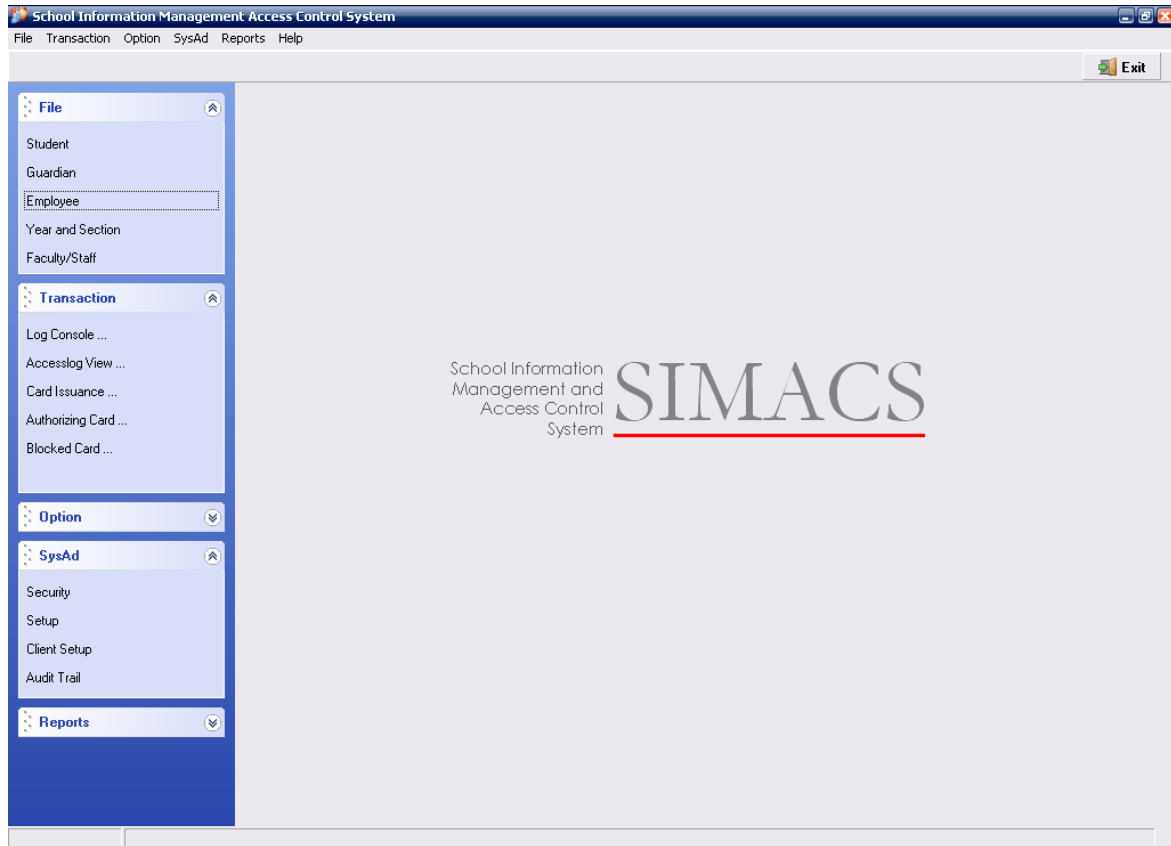
Description

The SIMACS is all embracing software that, as its name suggests, provides the management of the facility or building the means of monitoring and controlling of the events in various access points of the vicinity where scanners and readers are being deployed. The information that was captured and logged in SIMACS the owners, building administrator and operators provides the required level of service to their visitors or tenants in their security.

SIMACS provides and supports various devices in a mixed environment of deployment. It controls the devices from PC-base devices up to the autonomous IP Base Device and controllers. RFID cards and Smart cards, Biometrics and RFID Readers or scanners were the primary device used as a medium for verification and Identification. To date, SIMACS was successfully integrated to one of the leading SMS Platforms and Server. Thus SIMACS gets you to the next level of security thru SMS notification and messaging.

Recently, SIMACS was been deployed in a school for their student security and access control. The school deployment gives the parents of the students the advance notification thru SMS when their children arrives and leaves the school premises. It was also extended to employee to give their Human Resource Department the actual time in and out of their staff for their payroll and time keeping use.

SIMACS can be accessed thru Windows Application or via Web Browser. SIMACS is backed by a full-featured open-source database server "FirebirdSQL".



General Feature:

- Supports mixed device environment. From PC-base to IP Base Readers
- Centralized Smart Card Issuance Management
- Centralized Smart Card Blocking Management
- Centralized Access Logs
- Multiple Identification Function or Combination
 - Identification thru IP-base Biometric Device (PIN+FP)
 - Identification thru Smart-Card (SC+FP/SC+PIN)
 - Online Screen Identification – Actual personal Information from database
- Maintains Information for Employees, Visitors, Students, Fetchers and Guardian
- Access for Doors or Readers can be designated
- Short-Messaging-System (SMS) Interface
- Supports Contact and Contact less Smart Cards
- Supports interface to various turnstile devices and electronic door locks
- Provides Online Display
- All Access Logs are captured (True, Invalid, Override)
- Data can be transported to you any of csv, text, delimited files
- Server can be of Windows, Linux or Unix Operating System

Systems Feature:

Employee & Staff Management - The ESM module provides the minimum and correct registration of the employee and staff information. Personal, Photo, Employee Group and Address information are being captured on this module.

Student Management - The Student Management module provides for the correct registration of the students, parents information and guardians or fetchers, and ensures that his records are maintained in a safe and efficient manner for easy access by those who need such access. The module includes:

- Student Personal Profile
- Parents Information and mobile numbers
- Fetchers and Guardians Information with photo
- Student IC Card Information and Status
- Reference on Staff

Fetcher or Guardian – This module maintains the Personal Information including their latest photo. Contact Information. Card Issuance status and validity

Access Points or Gates – This module contains the device or reader parameters. It can also be referred as door or gate for convenience on terminology. SIMACS captures and stores this information on the access log for additional security.

Some of the Supported Devices:



Transactions:

Smart Card Issuance – Issuance type will be for Student, Fetcher/Guardian and Employee. Information maintains are the ff:

- Date and Time of Issuance (Data)
- Card Validity (Data)
- Gate Access Assignment (Function)
- Automatic update to the profile of latest card issued (Function)
- User or Issuer of cards stamped on the transaction (Data and Function)

Smart Card Blocking – Blocking of cards referred from the issuance module. Blocking of cards could be for students, fetchers or employee. Automatic blocking for invalid cards is being on done on the access module.

- Date and Time of Issuance is being captured
- User or Issuer of cards stamped on the transaction

Special Card for Authorization – Special Function cards are also being used in the system. This allows the security to have a secondary validation. In most cases, this function is used for pc-base reader with multiple in/out functions.

Card Inventory and Reports:

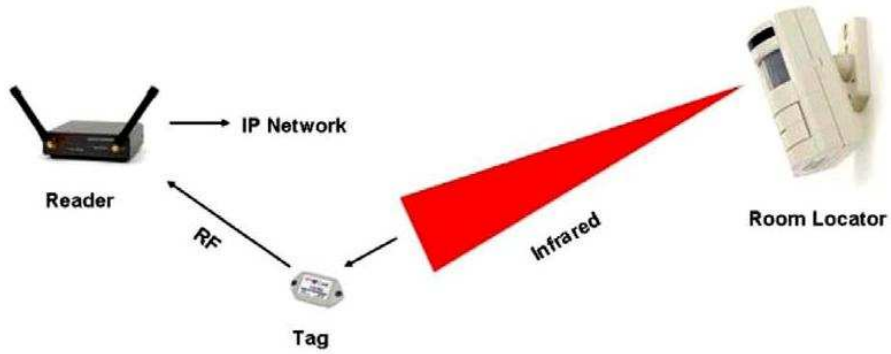
The system includes a comprehensive inventory system for IC cards that allows the user to monitor the usage and spoilage of the cards. Card monitoring could be of the following:

- Number IC Cards being issued by student
- Number IC Cards being issued to all students
- Consolidated reports of all cards being issued, blocked, reused for any period or date
- Number IC Cards blocked and used but not qualified

System Security

The system is designed to be secure. Each and every person who is required to use the system must be issued with a User Name and Password. All passwords are encrypted by an AES (Advance Encryption System). Individual Workstation profile is adopted for additional security. Automatic Log-off is being implemented to ensure the online users credential is protected. Changing passwords is automated on a scheduled basis and set to individual user profile. Built-in systems audit trail, a standard practice for any database application for security and investigation purposes.

RFID Application for SIMACS Typical Setup



RFID ID Badge & Security Systems



Library RFID Management System

