Deployment of an Advanced Building Access System

Installation of advanced door access system in a building/premise is no longer an option. It has become extremely important because it protects the company's profits by keeping revenue-generating equipment secure. A must-have tools and criteria for a building access system would include centralized management, detailed access transactions, advanced notification and credible verification method i.e. biometrics/smartcard. Having a good and reliable system also reduces the cost of managing remote sites, as the system allows the viewing and controlling of access remotely from a central terminal.

Unmanned building and premises are vulnerable to not only from strangers but more importantly from people that familiar with your premise such as employees, ex-employees, and outside contractors Basic security feature is not going to do the job. To effectively manage your sites, access should be restricted to authorized personnel only and security system must possess user-level access control complete with a log of every entry and exit.

10 Key Features of A Credible Building Access System

Centralized Management
Centralized management is where your building access system is manageable from a central terminal. With this, you can watch over and control your access points from a single monitoring platform, which also can be accessed remotely. This increases overall system effectiveness and reduces staffing requirements.

Biometrics/Proximity Reader Support
Proximity card readers or biometrics readers offer a variety of advantages over traditional keypads. Keycards cannot be shared with others as codes can be, and keycards are much better for use in hostile climates. A good access system should support a selection of user input devices, including proximity readers and keypads.

Detailed Logging
Your access system should log every entry to your sites. Knowing exactly who accessed your sites, and when they did so, is crucial the event of vandalism or theft.

Compatibility with Site Power
Your building access system should operate on site power, either battery or commercial. By using protected power, your system will still work during a commercial power failure.

Sufficient Size for Your Network
If you are going to incorporate an access system into a large network, it should support for at least 1,000 user codes/biometrics templates or keycards at each site, with support for at least 50,000 total codes or cards throughout the enterprise.
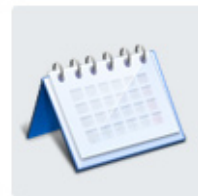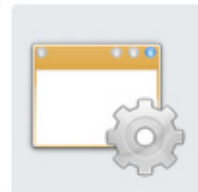
Access Scheduling
You should be able to define a weekly schedule for site access. This ensures that your sites can only be accessed when they should be.

Multiple Transport Options
Your building access system should support multiple paths for upstream communication. LAN and serial should be available.

Fault-Tolerance
A good system has a redundant user database. Individual sites must be able to operate independently of the master if communication is lost. The goal is to make the decision of access locally, then report to the master. By alleviating the reliance on the master, you can get fast access, even in the event of a communication failure.

Independent Door Control
Look for an access system that gives you the power to control each door at your facility independently. You might want to give many users access through the front door, but restrict access to a central area to just a handful of key staff. To do this, you must be able to control exactly which personnel can enter which doors.
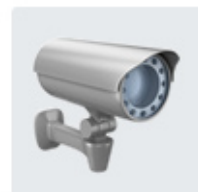
Video Surveillance
A complete network alarm management system requires more than just environmental and equipment monitoring. Security and personnel issues are also part of the complete picture. Video surveillance is especially useful when used in conjunction with a building access system. This will allow you to visually watch over your site.