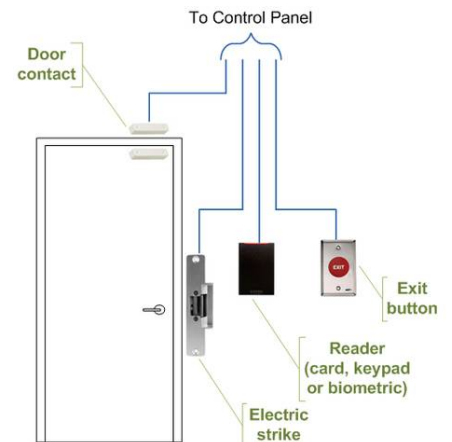


Important Considerations When Selecting.....Access Control

An **Access Control System** functions as the primary method to control access to your facility. When doors are locked, personnel can typically enter through an access door by presenting security credentials to a reader. If the credential registers as a “valid read”, the electrified locking hardware will be signaled to release the door lock for entrance. Below is some common security terminology used when referring to access control systems. If you are considering purchasing this type of security solution for your facility, we encourage you to review this information prior to making your decision.

Standard Door Configuration – A typical access control system door configuration consists of the following devices:

- Reader – Unit used to determine whether or not to grant access through presentation of security credentials such as a proximity card, keypad or biometric identifiers such as fingerprint, iris, or retina.
- Door Contact – Device installed in door frame to notify the system of door status (i.e. open or closed).
- Request to Exit – Device mounted on opposite side of door from reader to grant exit without requiring security credentials.
- Electronic Lock – Device mounted in door frame to prevent door from being opened.



Credential Type – Before the system will grant access to an individual, one or more security credentials must be presented to a reader. Common security credential types include proximity cards or keyfobs, which require a user to hold the credential near the reader but do not need actual contact with the unit in order to facilitate a valid read. Smart cards are the newest card credential technology, and allow data to be stored directly on the card. Data storage can include access control information as well as financial and personal records. Smart cards can be programmed to interface with a variety of systems and eliminate the need for a user to carry multiple cards to access a facility, purchase items, and perform other tasks.



Standalone Access Control – Type of access control system that controls a single door and does not share data with other door control units. These are common in smaller facility applications, and typically have fewer features than networks as well as less user capability.

Controller-Based Access Control– Used frequently in multiple door applications, this type of access control system is connected to a central control unit (usually a PC or server operating the access control system software) which allows an administrator to run reports and update user information.

Fail Safe/Fail Secure - Designation based on the non-powered state of an electronic door lock. A "fail safe" designation indicates that the lock is open (door unlocked) when power is absent. Fire code compliance often requires a fail safe lock to be used in certain areas. A "fail secure" designation indicates that the lock is "closed" (door locked) when power is absent.

Badging System –Refers to supplementary access control equipment required to print names, photos and other information on proximity cards used to access a facility. Badging is not required for your access control system, but it does offer an additional layer of security by providing security personnel with the means to visually identify the owner of an assigned proximity card.

Software Licensing – Many industry standard IP Video and Access Control security platforms often require annual software licensing subscriptions in order to provide access to manufacturer updates and technical support. These are valuable services that help to ensure the future viability and scalability of your system. Make sure you are aware of manufacturer software licensing requirements prior to selecting a security solution.



Scalability – When purchasing a security solution, consider potential expansion needs in the future. At this point you may wish to monitor only a portion of your facility, but perhaps a renovation or an increase in funding will give you the opportunity to add to your system in upcoming years. Planning for these needs will allow your integrator to provide you with the most cost-effective and flexible security solution.

Connectivity – Consider how you want to interface with your security solution. Do you want to be able to access it from a computer in a control room or on your laptop at home? Perhaps you want to log into the system on the go through a smart phone such as Android or iPhone? A variety of connectivity options are available for security applications, although features such as multiple workstation client and web client/browser based software options may incur additional costs. Also, some security solutions will not offer all connectivity options for certain operating systems, so it is important to discuss the operating system your facility is currently using (Windows, MAC, Linux) with your integrator.

