

# Criteria for selecting an access control system



Selecting the right access control system can be an exhaustive task. After all, there are hundreds of solutions on the market, all with distinct features. Determining the right solution will depend on a variety of factors such as the size of your business, budget, the number of readers you need, and your building's business objectives.

Whether you're working with a systems integrator, architect or researching on your own, there are a number of questions you can ask to ensure that the system you are implementing is right for you:

## How reliable is your access control system?

Electronic access control systems rely on various technology such as biometrics, Wi-Fi, NFC and Bluetooth. The problem is that these technologies require 24/7 uptime or some type of accurate reading in order for the system to work. However, reasons such as misread fingerprints, acts of God or random internet outages can cause the system to fail. As a result, most access control systems have at least some reliability issues, creating a poor user experience.

## Does the access control system integrate with existing security infrastructure?

Most buildings have some type of video surveillance in place to ensure employee safety and protect the business from theft. However, with the advent of video management systems (VMS), organisations can now perform more complex functions such as people counting, license plate recognition and even predict incidents before they happen. Having an access control system that integrates with your VMS enables businesses to operate their security operations more efficiently and collect more data. In addition, they can connect with other systems such as guest management systems and alarm systems.

## How does your system work with intrusion detection?

Many of the newer access control companies have the ability to integrate intrusion detection technology into their system. Intrusion detection allows companies to lock, unlock doors and rearm the doors all at once by using some type of credential such as a card, fob or even mobile device. This functionality prevents an employee from needing to lock every door in the office and setting an alarm before he or she leaves for the day.

## Can this system integrate with existing office automation functions?

Some access control systems have added intelligent automation to integrate seamlessly with various business apps and even devices. Adding this level of functionality enables businesses to use their access control system creatively for functions such as visitor management, lighting and room booking. As IoT-enabled devices shift from disrupting the home to the office, it will be important to look for solutions that can enable complete office automation.

## Will my employees be able to easily use this system?

While your employees are likely to welcome using their smartphones opposed to the burden of remembering a fob or key card, some technological upgrades will create added friction. For instance, many of today's mobile access control systems require the user to unlock their phone before using. Since this adds extra steps, users might simply prefer a more intuitive key card than smartphone credential technology. In addition, biometrics solutions require the user to have a clean fingerprint or line up their eyes directly with the reader. As a result, this can delay users by several seconds and create frustration. The ideal access control solution is one that doesn't require the app to be open, and/or the phone to be placed over the reader.

### How will a modern access control solution evolve with my business?

The modern office is constantly changing to adapt to the flexible worker. As millennials are now the single largest segment of today's workforce, and an even more technologically savvy Generation Z enters the workforce, employers can attract talent by implementing access control technology that allows employees to work flexible hours. In addition, companies need a solution that can work with various apps they are already using at work. In order to make these accommodations, businesses should invest in an access control system that has open APIs, is based on the cloud and integrates with the rest of the office. As the Internet of Things increases in popularity businesses should seek applications that maximize technology and are customisable to their employees' needs.

### What security features does your access control system have?

Problems such as cloning, lost/stolen access cards and reader vandalism are common problems in the access control industry. Any one of these problems can have a detrimental impact on your company's security. Leading access control companies are utilising multi-factor authentication to provide clients with an added layer of protection. This helps ensure that the user trying to unlock the door is truly who they say they are. In addition, your access control solution should have a back-end system that enables real-time monitoring to determine each instance of failed entries, ajar notifications and any other irregularities that occur at your office. Time based entry is another feature enabled by cloud-based access control.

### How does your solution work with controlling elevator and garage access?

In order to add an extra layer of security, buildings are starting to deploy access control systems in elevators and garages. In fact, several corporate offices now have smart "destination dispatch" elevators, which allow passengers to request a particular floor using a touchscreen or keypad. This ensures maximum efficiency and prevents overcrowding the elevator. As part of the added intelligence, elevators are also checking to make sure each individual has access to their respective floors. Garages, especially in urban communities are vulnerable to criminal activity without proper access control in place. If either of these requirements are important, ask your prospective vendor about if this functionality is available and figure out what sort of manual labor is involved.

### Can your system handle inclement weather?

Surprisingly, durability is not a key feature with many access control solutions. This can at times make readers malfunction in cold environments, rain or dust. You can ask your integrator if this system has an IP65 rating if you're planning to install your reader outside.

### What sort of mustering scenarios does your system handle?

Mustering is a powerful feature in the access control industry that allows admins to use access logs to locate people in a building or specific area. This capability analyses the logs to determine where a user is in the facility and can help with time and attendance tracking. A mustering system can use time logging to track a user's movement throughout the building by providing insights into where a user was at a given time. This is often valuable when a building administrator needs to track potential criminal activity or for safety needs.

Ready to learn how MJ Flood Security can help you and your employees enjoy both convenience and security?

Contact [sales@mjflood.ie](mailto:sales@mjflood.ie) or call us on 01 689 6390



[www.mjfloodsecurity.ie](http://www.mjfloodsecurity.ie)

**openpath**  
a Motorola Solutions Company