

# IPVM

## 2021

### ACCESS CONTROL TRAINING BOOK



# TABLE OF CONTENTS

Special For 2021: Coronavirus Articles.....	1
How Mobile Access Control Can and Cannot Help With Coronavirus.....	2
Hands-Free Bathroom Doors For Coronavirus Mitigation.....	12
Add Door Operators To Fight Coronavirus.....	18
Use Access Control Logs To Constrain Coronavirus.....	22
Life Safety.....	30
The Access Control Codes Guide: IBC, NFPA 72, 80 & 101.....	31
Building Occupancy Codes.....	41
Free Online NFPA and IBC Codes and Standards.....	49
Access Control ADA and Disability Laws.....	52
Standard for Access Control (UL 294).....	59
Fail Safe vs. Fail Secure.....	63
AHJ / Authority Having Jurisdiction.....	71
Doors & Locks.....	77
Door Fundamentals.....	78
Door Hinges.....	89
Specifying Door Locks.....	98
Door Swing.....	105
Maglock Selection.....	110
Selecting the Right Electric Strike.....	123
Electric Strike Installation.....	129
Access Control Request to Exit (RTE).....	137
Exit Devices.....	146
Door Closers.....	154
Door Operators.....	162
Door Position Switches (DPS).....	171
Lock Status Monitoring.....	181

Advanced Access Openings.....	189
Multipoint Lock.....	190
Glass Doors.....	197
Elevator Access Control.....	207
Turnstiles.....	211
Mantraps.....	223
Vehicle Gate.....	230
Credentials & Readers.....	240
HID vs NXP Credentials.....	241
Access Credential Form Factor.....	246
Hack Your Access Control With This \$30 HID 125kHz Card Copier.....	253
Vulnerability Directory For Access Credentials.....	259
Cracked 125kHz Access Control Migration.....	268
Selecting Access Control Readers.....	275
Multi-Factor Access Control Authentication.....	286
Biometrics Pros and Cons For Electronic Access Control.....	293
Fingerprints.....	301
Fake Fingerprints - Liveness Detection Solutions.....	312
Mobile Access Control.....	315
Keypads.....	325
Hotel Access Control.....	333
Controllers & Management Software.....	343
Access Control Door Controllers.....	344
Access Controller Software.....	358
Open Access Controller (Axis, HID, Isonas, Mercury).....	368
OSDP.....	374
Access Control Management Software.....	388
Securing Access Control Installations.....	393
Access Control Records Maintenance.....	401
Networks and Cable.....	407
Cabling.....	408
Wireless / WiFi Access Lock.....	417

Drain Wire For Access Control Reader.....	425
PoE Powered Access Control.....	431
System Design and Special Conditions.....	439
Access Control Specification.....	440
Access Control Mustering.....	456
Tailgating.....	462
The Passback Problem.....	471
Delayed Egress.....	475
Propped Doors.....	479
Access Visitor Management Systems.....	483
Time & Attendance.....	491
Access Control Job Walk.....	497
Hazardous & Explosion Proof.....	508
"Future-Proofing".....	516

# **Special For 2021: Coronavirus Articles**

# How Mobile Access Control Can and Cannot Help With Coronavirus

With coronavirus concerns continuing to rise, many access control companies have pitched mobile access control as safer but how much are they? And what should be done?



We examine:

- Door Operators vs Mobile Access
- Coronavirus pitches from Openpath, BluBOX, and ZK Teco
- Feedback from HID, Farpointe Data, ZK Teco, and others
- Benefits of mobile access control for coronavirus
- Fingerprint reader issues
- Limitations and issues that remain for mobile access control
- Outlook on how coronavirus will impact mobile access adoption

## **Executive Summary**

While mobile access control can incrementally reduce the potential for touching surfaces, entering still overwhelmingly requires people to touch the door handle or door to open the door. As such it might marginally be safer but bigger risks still remain.

Nonetheless, given the heightened awareness of the risks of touching things and high emotions currently, we expect that mobile access control will benefit.

## **Dirty Door Handles Remain**

For the vast majority of access openings, the reader is used to unlock a door, but the user must, in turn, open the door using a commonly touched door handle.

This means the potential to pass contagions between users still very much exists.

For example, the [CDC specifically recommends 'cleaning and disinfecting' door handles](#) to combat Coronavirus.



If complete non-contact with access controlled doors is desired, the opening must be equipped with an [automatic operator or opener, as we cover in this tutorial](#):

**IPVM**

## DOOR OPERATORS ACCESS CONTROL TUTORIAL



Perhaps those devices will see an increase in deployment as they can clearly reduce contact and spreading viruses.

### Coronavirus Pitches From OpenPath, BluBOX and ZKTeco

Mobile access [Openpath](#) sent an email promotion emphasizing the coronavirus hygiene benefit of 'hands-free unlock' with 'no need to touch the reader' using the platform's app-based unlock button and touchless 'wave' feature to unlock doors even with phone stowed and untouched in a pocket or purse.

## COVID-19 Response and Useful Openpath Features for Flu Season

Openpath Security <no-reply@openpath.com> [Unsubscribe](#)

to brian ▾



As the community works together on the COVID-19 prevention and mitigation plans, in the midst of cold and flu season, we would like to express our heartfelt thanks to all parties on the forefront of helping to combat this pandemic. We must look out for one another, [take precautions](#) and err on the side of safety.

With a number of customers enacting remote working policies or considering such a move, these steps might present organizational and administrative challenges for your business. In that light, the Openpath platform has some features you might find helpful:

**Hands-Free Unlock** - No need for your hands to touch the reader in order to unlock an entry. The following methods can be used instead:

- Unlock the door directly from the app on your phone.
- Unlock by simply waving your hand in front of the reader.
- Touch the reader with a covered body part such as an elbow, an inanimate object such as your phone.

And BluBOX [tweeted](#):

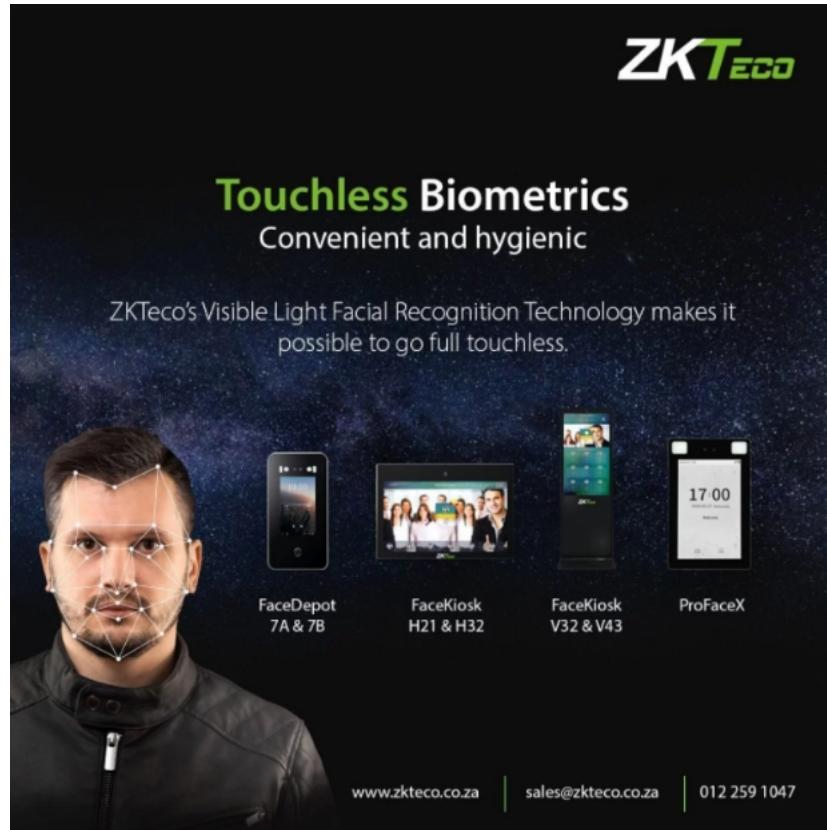
**BluBOX Security Inc.™** @BluBOXSecurity · Mar 13  
The COVID-19 outbreak continues to be on top of everyone's mind. Readers that are hands-free such as the Person Reader provide a healthier, more convenient & secure approach to access control. #accesscontrol #security #prevention #coronavirus #coronavirusoutbreak #covid19

### Go Hands-free with The Person Reader

- All-In-One Intelligent Reader, Intercom, Camera and Visitor Entry Device
- Multi-biometric, Multi-factor Identification Device with Liveness Detection
- Fast, Robust, Accurate and Easy to Use
- Uses any combination of Appearance, Voice, Name, HID Prox/iClass/Bluetooth, MiFARE, Barcode/QR Code, Digital Credentials or PIN



Plus, [ZK Teco SA](#) touting the hygienic advantage of their face readers:



#### Feedback From HID, Fairpointe, ZkTeco, Others

However other mobile access vendors were less likely to advocate mobile as a coronavirus solutions.

Several told us in emails that while their company's mobile offerings have usability advantages, they will not tout their mobile as being safer or more hygienic than traditional contactless credentials.

For example, [HID Global](#) told us that even traditional credentials are typically 'non-contact' when used:

The majority of our current and traditional reader/credential offerings (including mobile access) are well-known for being contactless but are not being promoted specifically as a solution in

response to the coronavirus. By definition, these solutions do not require the user to touch anything (other than their credential) to successfully authenticate.

And [Farpointe Data](#) commented:

I'd hesitate Farpointe trading on mobile being a 'healthier' option. Seems to me the mobile phones themselves are suspect, as they are in constant contact with our faces, ears, lips and hands (Leads me to think of my teenagers' phones!). Also, after access is granted the end user typically needs to pull or push the door open, meaning they need to touch the handle that everyone else has touched. Germs from the phone can be transmitted to the hand, then to the door handle, then to the next user, and so on.

Other vendors told us while they see their mobile offerings as indeed healthier, they will not make those claims in company sales and marketing out of concerns of 'poor taste':

We do believe that mobile access is better from a disease prevention perspective than things like finger print readers or touch readers that require physical contact. Its benefits over the more popular contactless card method is harder to argue.

However, we think it is poor taste to promote small improvements in hygienic practices that a product could support in the face of what will certainly be a globally catastrophic event in which many thousands if not millions of people will die, so we do not plan to use this in our product positioning.

However, other vendors noted that overall interest in mobile has increased in recent weeks, and mobile and face recognition access allows businesses to provide the safest solution to employees.

For example, [ZK Teco USA](#) told us:

Today with every news station covering the coronavirus, no business owner can afford not taking every conceivable precaution to limit exposure of the virus to their customers & employees.

Prior to the coronavirus outbreak, we'd primarily promote the enhanced security and convenience which only biometrics provides . . especially touchless biometrics (inc. face & palm).

However today . . if given the choice between touch and touchless security technology . . why take the chance on "touch" technology when "touchless" technology provides a much faster, safer (and hygienic) user experience.

Even before news of the virus outbreak, we've been seeing an increasing demand for both our mobile (Bluetooth) and biometric readers.

I believe most of this growth is fueled by the growing dependence people have for their phone. Most all phones now have Bluetooth and biometric sensor to unlock it.

### **Fingerprint Reader Cleaning/Disinfecting Recommendations**

Fingerprint readers are likely to be harder hit, as we discussed here - [Will Coronavirus Kill Fingerprint Readers?](#)

For example, ZK Teco USA [recommends](#) to clean the surface between each use:

To help prevent the spreading of COVID-19 and other bacteria & viruses, ZKTeco USA recommends taking extra precautions by cleaning your fingerprint reader after each use.

This is obviously impractical and we expect many users to abandon fingerprint usage.

## **Benefits of Mobile For Coronavirus**

Indeed, we see two benefits of mobile access Recap what benefits for mobile access over conventional access:

### **Personal Phones Are 'Social Distancing' Compliant**

In terms of isolation, using a phone app to unlock doors without gathering around readers where other users are gathered provides further distance protection against passing Coronavirus to others.

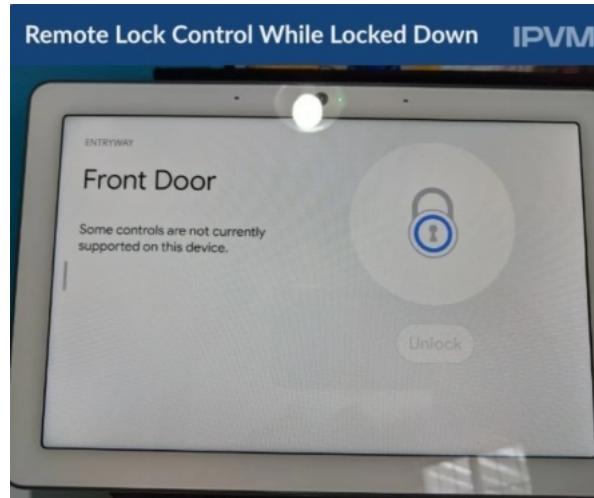
For example, mobile apps can permit users in cars to activate openings while still seated in vehicles. The same distance flexibility allows users to be many feet away from other users when unlocking a door:



### **Remote Access/Unlock Support**

Another related advantage is doors can be locked/unlocked from a great distance, even users who may be working from home who still are responsible to grant access for deliveries or building checks.

In the same manner as access can be granted from a desk computer or tablet from deep within a facility, the same approach applies to someone that may be many miles away:



### No Contact With Cards/Fobs Anyway

Even for many 'non-mobile' access systems, physically touching credentials to readers is not typically required with common credential formats:



While carelessness may cause users to brush their credentials into contact with readers, providing an avenue for contagions to pass between surfaces, designs allow for airgap isolation between user credentials and common readers.

## **Outlook**

While we think mobile access control will benefit from this, for users that really want to radically reduce contact and risk for infecting others, [implementing door operators](#) is a much more direct solution.

Combining that with mobile access control can provide a significantly enhanced solution.

# Hands-Free Bathroom Doors For Coronavirus Mitigation

Coronavirus has increased concerns about picking up germs, especially from bathrooms.

Instead of cleaning handles after every user, companies have started pitching interesting, but costly, automatic operator solutions for hands-free door operation.



We examine one manufacturer's 'hands-free' pitch, break down the costs, look at similar solutions, and discuss other non-powered solutions.

## Door Operators To Fight Coronavirus

The concept of using operators to automatically open doors to stop the spread of germs is not new - a benefit we discussed in [Add Door Operators To Fight Coronavirus](#).



## IPVM

### ADD DOOR OPERATORS TO FIGHT CORONAVIRUS

However, these devices have been typically installed on perimeter/high volume doors but not bathroom doors.

But Coronavirus could be changing that.

#### Using Door Operators On Bathrooms

Hardware company [SDC is touting](#) a kit solution packaging a door operator and two hands-free buttons for retrofit on doors where 'contamination control is required' like bathrooms:



In most situations, this system is likely to work well because it truly is 'hands-free' to trigger door opening from either side, and the [automatic operator](#) is specified to push or pull open the door regardless of [door swing](#).

## Hands-Free Door Releases

Making operation 'hands-free' is taking the approach a step further. This solution uses equipment that has been used in access and door automation for many years.

Hands-free/germ-free operation is possible because SDC specifies using 'No Touch' activation buttons. With those users '[wave](#)' hands in front of the IR sensor (instead of physically touching a push-button) and the operator is triggered to open:



This system is not connected to an access system, nor are traditional readers/credentials used, so it is not designed to keep areas secure.

### SDC's Operator Solution Is Costly

With the pandemic changing the market for operators, new lightweight types of doors (like bathrooms) using smaller or less powerful operators are required than heavy-duty \$3,000+ units driving perimeter doors. But even the light-duty units (like SDC's) are still pricey add-ons.

The price of using SDC's 'hands-free' kit is ~\$1,400 in hardware components alone. Street prices include one AutoEntry Opener at [~\\$1,300](#) and two Hands-Free Release Buttons at [~\\$100](#). That price does not include wire, power, and install costs which will typically add multiple hundreds, perhaps even thousands, more.

However, given the typical prices of lightweight operators and releases, SDC's kit is priced at the lower end of similar options (often \$2,000+ for a kit with operator and release buttons).

## **Competitive Kits Priced Higher**

Other operator kits are generally priced higher than SDC's. For example, [Norton's 5800 series kit runs ~\\$2,150](#) and includes two wireless buttons that must be physically pressed to open.

While the wireless buttons are less expensive to install and use no wire, the cost of cleaning the contact surfaces and changing batteries drive operation expenses higher just than the ~\$750 greater asking price.

## **Doorless Bathroom Openings**

Another method to avoid sharing germs on dirty door handles is the elimination of bathroom doors altogether.

Examples are common in public buildings, where the physical layout of the bathroom and wall placement provide user privacy without requiring the use of hinged openings:



We expect a mix of more doorless bathrooms and more hands-free doors. For new, large buildings and public restrooms designed to handle high user volumes, doorless bathrooms will

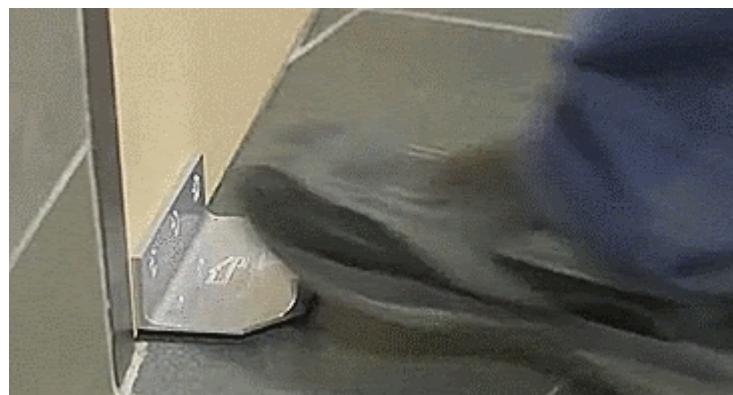
fit best. However, considering the cost and space required for retrofitting in existing buildings, we expect other 'hands-free' solutions to be a less expensive and less disruptive option.

### **Manual Opening 'Hands-Free' Alternatives**

However, there are non-automated options for 'hands-free' door opening. We examine several in a recent discussion: [Anyone Using This Anti-Germ \\$30 Door Opener?](#)

These options generally use a modified type of door pull that use feet or forearms to open doors but do not need users to grasp them with hands.

One example is this [\\$30, foot-operated lever, the StepNpull](#), where users pull a door open with their feet:



[Click here to view the animated gif on IPVM](#)

However, these solutions are not typically ADA compliant and may increase the risk of user injury/slips and falls, where more expensive powered door operators will not.

### **Integrator Opportunity**

Considering the dealers of lightweight operator kits like SDC's are often integrators, there will be opportunities to pitch operator kits as 'hands-free' solutions for bathroom and other interior (non-security) doors.

However, those same doors are not likely candidates for regular access control either. Especially for bathroom doors, the purpose of the operator is health-related, not security, so adding access is unlikely.

### **Vote**

Tell us what you think:

[Click here to view the poll results on IPVM](#)

## Add Door Operators To Fight Coronavirus

IPVM recommends that integrators advocate and end-users consider adding door operators to fight the spread of coronavirus.



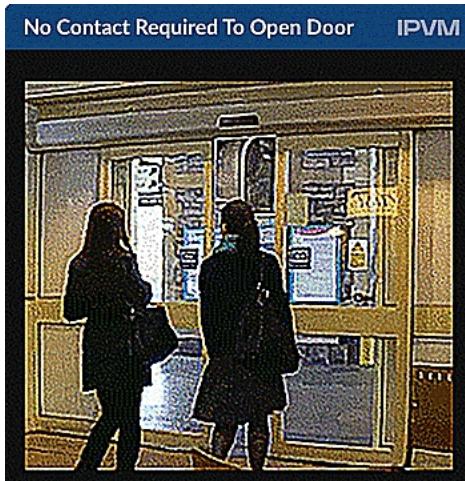
This delivers mutual benefits - providing business to integrators in a slowdown and improving the attractiveness and health of customers coming to businesses.

### Why End Users

While [mobile access is getting a lot of attention](#) for its potential to help with coronavirus, the biggest health problem in access control is opening doors, in particular grabbing the door handle



By contrast, door operators allow people to enter a business without touching anything:



[Click here to view the animated gif on IPVM](#)

The problem is that lots of businesses, especially smaller ones, do not have door operators. In the past, it was an expense that could be viewed as overkill but now it is an investment in reducing the spread of coronavirus.

### Why Integrators

Many integrators are struggling to find work as customers have cut back amidst shutdowns and overall uncertainty. However, end-users are still purchasing heavily for products or solutions that help fight against coronavirus (witness the surge in thermal fever detectors).

While those things are risky, door operators are straightforward. They are an established technology.

Integrators have largely ignored them in the past because they have been so busy just with core video and access projects.

But now, many integrators are looking for ways to not furlough or layoff employees.

Enter door operators.

### **Door Operator Dos and Don'ts**

A few things to keep in mind for integrators who have not historically installed door operators:

- *Have Door and Lock Knowledge:* The complexity of door operators is high compared to simple locks. In general, the integrator needs to understand which [type of door](#) is being fitted, but also things like [Door Swing](#), the application of [ANSI A156.19 Standards](#), [Accessibility Laws like ADA](#), and even other door hardware that is installed on the door like whether compatible [Locks](#), [Hinges](#), [Exit Devices](#), or [Delayed Egress](#). Installing an operator often replaces existing access locks and hinges, and as noted in our [Door Operators Access Control Tutorial](#), integrates the controller to the operator instead of locks.
- *Planned Site Interruption:* In short, when an operator is installed or serviced, the door should not be used by building occupants. The scheduling of operator work can be disruptive to a business and often requires agreement and permission from many different groups, especially in a larger commercial or multi-tenant office space.
- *Expect Frequent Maintenance:* Automatic operators are generally built to last hundreds of thousands of cycles, but they typically have many parts and sensors that must be properly adjusted to avoid becoming barriers. Rapid service is key as worn/broken operator parts must be repaired/replaced urgently or else the opening is not secure. In many cases, operators are used on [Emergency Egress](#) openings, and the operator

mechanism and opening might require frequent maintenance to ensure the code compliance and safety of a building.

And a few integrator operator 'don'ts':

- *Ignored Guards and Railings:* In many cases, the operator install does more than modify the door, but also the area around the door on both sides. 'Extra' safety items like adding handrails, finger/pinch guards, and moving potential interference items like bulletin boards or video PVMs away from the automatic travel of the door is often forgotten by installers.
- *Neglected Signage/User Training:* While door operators are easy to use, occupants may need training on how to disengage doors for emergencies and the limits a door can swing without damage. Beyond that, hanging signs that display which side of a door is automatic and which direction it swings can prevent injuries.
- *Forgotten Backup Power:* Users can grow to expect powered operation so quickly, it is a big operational and security issue when power fails. Adding operators to available backup power systems to ensure continued operation and locking when main power fails is often overlooked by installers.

## Outlook

If you are an integrator looking for immediate business, contact end-users and pitch them on door operators. It is highly relevant to pressing needs and gives a valid reason to contact end-users and can generate business in a challenging time while helping these customers get back to business themselves.

## Use Access Control Logs To Constrain Coronavirus

Access control users have included capabilities that are not commonly used that can help zero-in and discover potential Coronavirus hotspots in a facility: system activity logs.



Getting this data requires tight access system configurations, which can give integrators an opportunity to consult or sell end-users on optimizing their systems and using access logs.

Inside this note, we discuss how to do this on any access system and which data is needed to make it happen. We also examine automated exposure reports from Genetec and Detrios.

### Risk Management Especially For Critically Open, 'Essential' Enterprises

With Coronavirus, while many shuttered sites have employees working from home, other 'essential' facilities cannot close, like clinics and hospitals, food and provisions business, and critical infrastructure.

For these 'essential' facilities, knowing who goes where and who they have potentially interacted with becomes especially valuable for determining risk and where to direct disinfection and cleaning first to stop the spread.

## Access Systems Already Record User Interactions

While many end-users are considering spending heavily [on thermal technology to combat Coronavirus](#), there is a good chance they already have an important tool not being put to full use: access control logs.

Using access logs, specifically to find out where people have been and who they have been in contact with helps avoid the rash, inefficient, and costly course of quarantining all workers and cleaning up an entire facility, especially for mission-critical buildings like hospitals.

Rather than issuing a disruptive 'lockdown/no contact' policy for everyone that may limit or restrict key assets and personnel, cross-referencing the movement and interactions of an infected individual offers a more selective and targeted path for countermeasures.

Most access systems include a report like this example, that shows where badges are used on specific readers/ locations in a facility:

Access Logs Show Where Users Travel IPVM						
		Report				
		Report				
		Report				
ReaderID	Card NO	ConsumerNO	User	Dept	Date/Time	Addr
105	18016105	1	Hellen	Sales Dept/Oversea Marketing	2011-04-29 15:08:16 Friday	Entrance Door In
104	20007405	2	Jack	Sales Dep	2011-04-29 15:07:52 Friday	Meeting Room Door In
103	18013377	6	Eric	Sales Dept/Oversea Marketing	2011-04-29 15:07:50 Friday	Meeting Room Door In
102	18013699	5	Lucy	Sales Dep	2011-04-29 15:07:49 Friday	Meeting Room Door In
101	3544172	4	Sharon	Product Dep	2011-04-29 15:07:48 Friday	Meeting Room Door In
100	18016105	1	Hellen	Sales Dept/Oversea Marketing	2011-04-29 15:07:47 Friday	Meeting Room Door In
99	20007405	2	Jack	Sales Dep	2011-04-29 15:07:43 Friday	HR In
98	18013377	6	Eric	Sales Dept/Oversea Marketing	2011-04-29 15:07:42 Friday	HR In
97	18013699	5	Lucy	Sales Dep	2011-04-29 15:07:41 Friday	HR In
96	3544172	4	Sharon	Product Dep	2011-04-29 15:07:39 Friday	HR In
95	18016105	1	Hellen	Sales Dept/Oversea Marketing	2011-04-29 15:07:38 Friday	HR In
94	20007405	2	Jack	Sales Dep	2011-04-29 15:07:33 Friday	Manager Room Door In
93	18013377	6	Eric	Sales Dept/Oversea Marketing	2011-04-29 15:07:30 Friday	Manager Room Door In
92	18013699	5	Lucy	Sales Dep	2011-04-29 15:07:29 Friday	Manager Room Door In
91	3544172	4	Sharon	Product Dep	2011-04-29 15:07:26 Friday	Manager Room Door In
90	18016105	1	Hellen	Sales Dept/Oversea Marketing	2011-04-29 15:07:24 Friday	Manager Room Door In

Using reports to guide response permit focused and narrow reactions to clean/disinfect specific areas promptly and test a narrowly identified group of people.

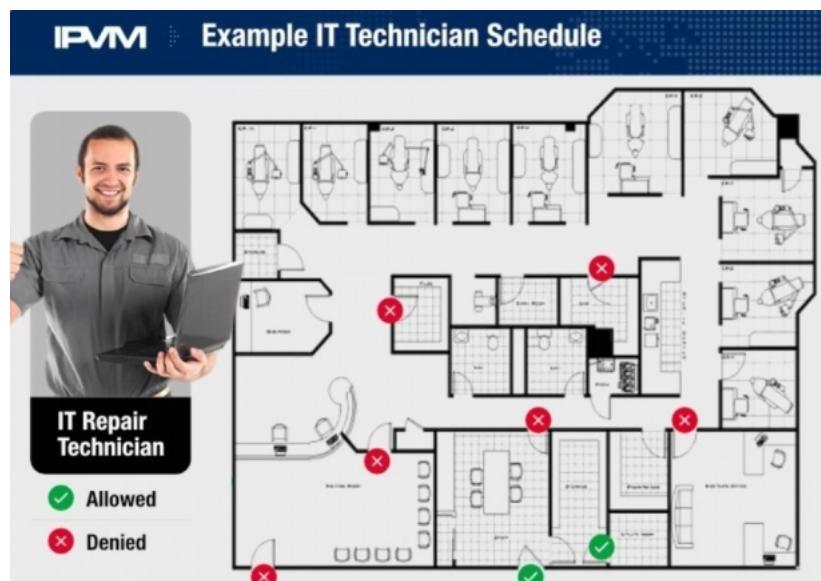
Being able to closely monitor a smaller number of people with elevated risks than rashly lock down an entire potentially vital facility helps avoid unneeded anxiety among employees.

Log checks also reduce the daunting task of disinfecting entire campuses and monitoring huge populations to just a few strategic zones.

### Access Levels Sequester Risk

A key benefit of access controls is [Access Control Levels and Schedules](#) that can tightly define where a particular person is allowed in a facility.

Like this example, 'IT Tech' from that guide, the employee is only allowed access via one door and a computer room. They lack permissions to enter/interact with other areas:



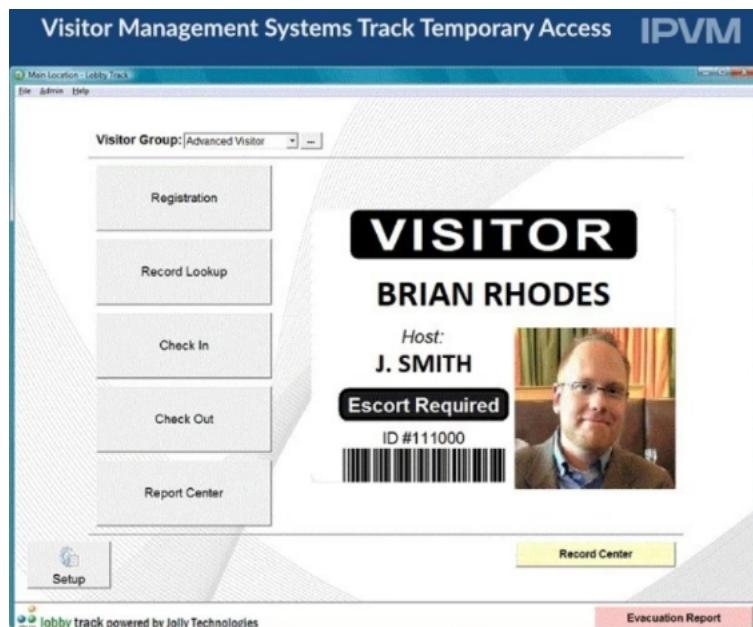
Using '[levels & schedules](#)' means employees are only given access to areas they need.

In the example above, for a potential impact like Coronavirus, if another non-IT employee elsewhere in the facility gets sick, but there are no logs showing their interaction with or travel into areas occupied by this example worker, undue intervention can be ruled out.

## Visitor Management System Data Tool

An expansion of those logs to non-permanent credential holders, even site visitors, can be achieved through using [Access Visitor Management Systems](#).

The circumstances of tracking individuals in a facility or campus and who they interact with is essentially the primary goal of the system:



Again, rather than a potentially unguided and wasteful 'global quarantine' facility-wide response that may outright miss visitors or contractors like delivery workers, visitors management systems help narrowly define the most at risk for infection.

## Multi-Building Visitor Management

Especially when visitors enter different buildings on a campus, like package delivery or medical couriers, being able to quickly determine everywhere an infected person has been is a benefit in dealing with potential exposures.

## **Risk: Potential Exposures Can Be Unlogged**

These reports should be used as general guidelines for Coronavirus infection risks, but these reports are only partial indicators because infections can happen without the access system logging it.

A weakness is that if access users are infected but are contacting people in a large group occupancy space they can potentially infect many without sharing doors, elevators, or readers at all.

In other cases, if infected users [Tailgate](#), use [Passback credentials](#), or otherwise undermine existing access controls and enter an area or contact people outside of the system's purview, this method will not detect it.

## **Integrators Can Help Train/Inform**

[Many integrators are struggling](#) to find work as customers have cut back amidst shutdowns and overall uncertainty, but training how to use these systems can be the right details at the right time for end-users countering Coronavirus.

Much of the data already collected by default in an access system may be unknown or not realized by end-users unless integrators tell or show them how to use it.

Training end-users how to use this data has not been a priority in the past, but now preventing the entire closure of a facility versus the isolation of just a few people might be operationally valuable detail that Integrators can pitch to end-users being able to collect.

## **Using Access Logs Against Coronavirus**

A few things to keep in mind for integrators proposing these as a potential Coronavirus risk management tool:

*Eliminate Flat User Systems:* Keeping people out of places they do not belong requires users to configure their access systems. If users opt for a 'lazy' or 'flat' simple access system that gives every cardholder into any door as they please, the benefits of reports are not possible or are greatly reduced.

If users are using 'flat' configurations, fixing it becomes the first step an integrator can pitch to help, even performing the work [via Remote Access](#).

*Garbage-In, Garbage-Out:* If end-users do not [Maintain Access Control Records](#), the underlying system is corrupted with bad or outdated information. The system becomes significantly less valuable and perhaps even worthless.

*Tailgating Risk:* Another enemy of activity log accuracy is the possibility of a single user holding a door open for multiple people entering or exiting an area. This prevents an access system from 'controlling' access at all. We note the full scope of the issue in [Tailgating: Access Control Tutorial](#) and discuss how otherwise polite gestures can actually be a serious security threat.

*Uncontrolled Doors:* Typically, not every door is included in an access control system, and due to availability or proximity to other uncontrolled openings. The risk of using these doors means the access system could be working perfectly but not satisfying the intended goal of keeping a facility secure and potentially exposed or infected people can enter an area without visibility of the system.

If, during log audits, it becomes clear that an uncontrolled door is putting an entire facility at risk, system expansion work becomes an obvious and easy upsell.

### **Genetec Synergis 'Proximity Report' Free Macro**

Some access providers like Genetec have begun offering customized report tools to automate potential exposures. For example, with the '[Synergis Contagion/Proximity Report](#)', users can:

Generate a Synergis proximity report to investigate who might have been in contact or in close proximity with a specific individual within a certain time range.

Genetec users create this report by creating and configuring a free macro in Security Center.

Genetec confirmed to us that the report may not indicate all potential Coronavirus interactions because it monitors only the portions of a building that are access-controlled:

The report is meant for passages, including doors, elevators, turnstiles, etc.

However, Genetec emphasized the operational value of just that data:

Even though the report does not target large spaces, the fact that we can identify individuals entering those large spaces through certain passages does permit us to narrow down the potential people who may have had contact with someone that was contaminated, and advise them as needed.

Once specific people are known to have tested positive, a report of names of users interacting with the same openings/readers/elevators within a defined time period is generated:

Genetec Contagion/Contaminant Proximity Report		IPVM
A	B	C
1 Cardholder:	Mark Black	
2 Dates searched:	2020-02-27 13:50:00 - 2020-02-27 12:00:00	
3 Time window:	30 minutes	
4		
5		
6 MTL-AN-02 N200A-First Main Door		2020-02-27 15:56
7		
8 Andrew Smith		2020-02-27 14:25 +00:29:19
9 Brandon Miller		2020-02-27 14:21 +00:22:54
10 Sylvia Benson		2020-02-27 14:19 +00:23:10
11 Michael Adams		2020-02-27 15:53 -00:02:55
12 Steven Wood		2020-02-27 15:52 -00:03:37

### Detrios COVID-19 Exposure Report Tool

Another example from [Detrios](#) offers a similar type of activity report for no cost potentially applicable to a number of access systems including AMAG, Avigilon ACM, Honeywell ProWatch, LenelS2, RS2, and Software House.

The tool generates an activity report using the same data to determine potential infection risks of others in a building:

Time frames can be specified before and after a COVID-19 positive individual entered an area. Administrators can also receive a CSV export of those potentially exposed to COVID-19, with the ability to obfuscate COVID-19 positive or exposed individuals' names, to protect people's identities and calculate the magnitude of exposure.

The tool is [no cost when using Convergint's](#) Professional Services Group.

## **Outlook**

If you are an integrator looking for business, contact end-users and pitch them on training how to use logs, tightening up access levels, and setting up visitor management to help constrain infection risks.

A review of user's systems and access data will likely present new opportunities or uncover gaps for using the system.

Besides being useful in keeping 'essential' sites open, it can help manage the risk of Coronavirus exposure among workers. It also a valid reason to contact end-users and can generate business in a challenging time.

# **Life Safety**

## The Access Control Codes Guide: IBC, NFPA 72, 80 & 101

For access, there is one basic maxim: Life safety above all else. But how do you know if all applicable codes are being followed?



While the basic maxim is simple to understand, many potential variations of rules exist, and access control professionals must understand them and how they apply.

In addition to looking at why codes are necessary, we examine the major codes dictating access control work including:

- IBC: International Building Codes
- NFPA 72: Fire Alarm
- NFPA 80: Fire Doors
- NFPA 101: Life Safety

This guide also provides the three steps needed to find which code applies to an opening, how to find local exceptions to broader codes, and which specific door functions impact code application.

## Why Classification Is Necessary

Unfortunately, a history of tragedies and deaths are the reason access codes are needed.

In the US, disasters like NYC's 1911 [Triangle Shirtwaist Fire](#) (killing nearly 150) drove the importance of properly operated and designated egress routes in a structure, eventually resulting in [the NFPA developing modern life/safety codes as a direct consequence](#):



Modern access codes are designed to make identifying critical protection areas easier, condensing egress requirements for even complex subsystems like physical access to simple rules.

## The Major References

While a substantial number of codes are used worldwide, many authorities draw code intent from a few 'model code' references. We cover each of these types in detailed sections below.

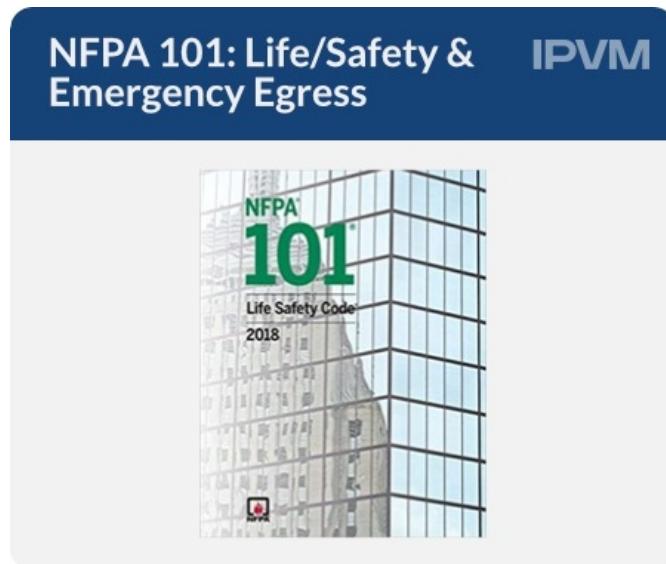


For access to the model codes used in many parts of the world and USA, see our: [Free Online NFPA, IBC, and ADA Codes and Standards](#).

However, this is not a comprehensive list, and other sources may be applied locally for access control systems, including legacy BOCA codes, [ADA](#), and Government Department or Military Jurisdiction codes.

## NFPA 101

The official 'Life Safety Code' is the most widely used source to protect people based on building construction, protection, and occupancy ratings.



While NFPA 101 is comprehensive, the most relevant passages for access control include:

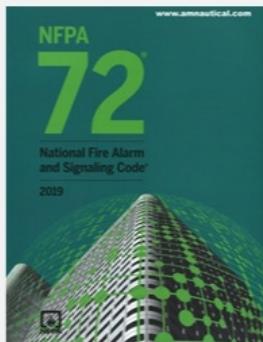
- NFPA 101: 'Electrically Controlled Egress Doors' (2015, 2012: 7.2.1.5.6; 2009: 7.2.1.5.5)
- NFPA 101: 'Releasing Devices' (2015, 2012: 7.2.1.5.10-12; 2009, 2006, 2003: 7.2.1.5.9 - 7.2.1.5.11)
- NFPA 101: 'Access Controlled Egress Doors' (7.2.1.6.2)

Specifically, requirements like [Access Control Request to Exit \(RTE\)](#), [Exit Devices](#), and [Delayed Egress](#) foundationally conform to NFPA 101.

## NFPA 72

Created for Fire Alarms, this code is sometimes cited in electronic access control because of the special integration required between the door locks and the fire alarm system.

## NFPA 72: Fire Alarm Code IPVM

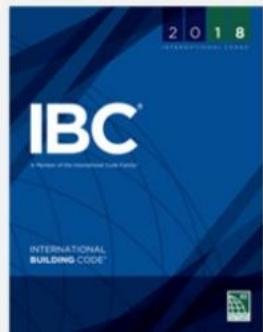


In general, this code is the foundation of requirements that doors must release when fire alarms or smoke detectors go into alarm.

## IBC: International Building Code

The IBC, published by [the International Code Council](#), is essentially a guidebook for designing and engineering safe buildings.

## IBC: International Building Code IPVM



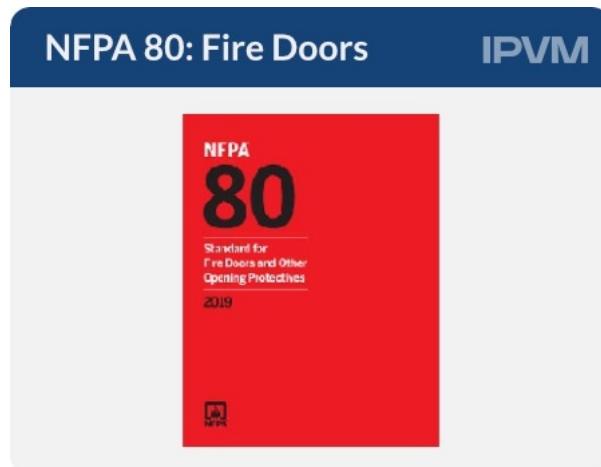
If not observed directly as the authority, then whatever resulting codes that do have authority take guidance from the source.

- IBC: 'Door Operations' (2015: 1010.1.9; 2012, 2009: 1008.1.9; 2006, 2003: 1008.1.8)

- IBC: 'Sensor Release of Electrically Locked Egress Doors' (2015: 1010.1.9.8; 2012: 1008.1.9.8; 2009: 1008.1.4.4; 2006, 2003: 1008.1.3.4)
- IBC: 'Electromagnetically Locked Egress Doors' (2015: 1010.1.9.9; 2012: 1008.1.9.9; 2009: 1008.1.9.8)

## NFPA 80

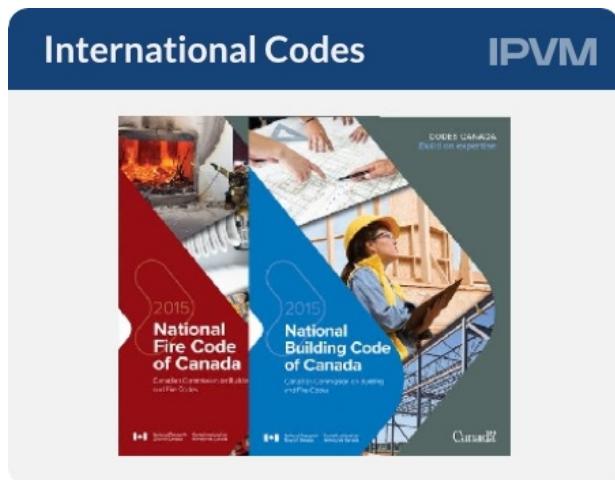
Specifically, this code examines Fire Doors and how they are properly used for protection in a building.



In many cases, these door types are also slated to become access-controlled openings, and the 'Locks or Latches (6.4.4)' section describes which modifications are permitted for access use without voiding their fire door ratings.

## International Codes

Because they are the highest default authorities if no other codes are cited they become the defacto regulations governing access control in the US.

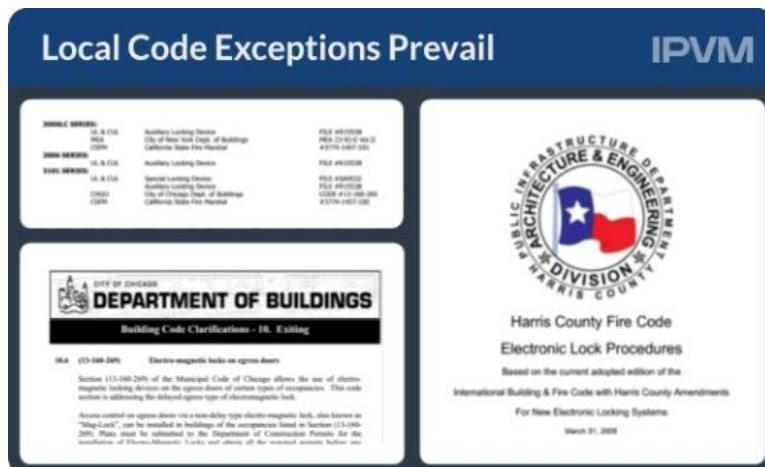


For example, in Canada, many model codes for access are based in the 'National Building Code: NBC'. Commonly cited codes are found in: 'Door Release Hardware (2015, 2010: 3.4.6.16; 2005:3.4.6.15)'

## **Local Code Exceptions Take Priority**

Exempted or municipal-specific codes are frequently ratified by local Authority Having Jurisdiction (AHJs), and it is the responsibility of access control designers to determine if local regulations impact what is normally allowed in model codes.

The image below details examples of local code exceptions that must be obtained through the local AHJ's office:



However, even when local exceptions exist, the general intent is the same: life safety must be preserved.

Rather, in no circumstances; normal operation, emergency condition, or even equipment malfunction, can a door prevent an occupant from escaping the premises.

## How To Determine Which Codes Apply To An Opening

In order to establish which access codes apply to a specific opening or door in a project, the three steps below will return the answer:

1. Determine Prevailing Model Code
2. Building Occupancy Codes
3. Establish If Opening is Emergency Egress

### Determine Prevailing Model Code

If not known, the first step is to determine which model codes and versions apply to a project.

There are [multiple free online resources](#) that list applicable codes and even whom [the AHJ is](#) for an area.

The screenshot shows the IPVM CodeFinder interface. At the top, it says "Researching Model Code Applicability Online" and "IPVM". Below that is a navigation bar with tabs: SELECT TOPIC, BUILDING AND LIFE SAFETY (which is selected), ELECTRICAL, EMERGENCY RESPONSE, FIRE PROTECTION SYSTEMS, and INDUSTRIAL HAZARDS. A search bar is also present. The main content area shows a map of the United States with a red overlay for Oklahoma. A callout box on the map specifies "NFPA Code-finder", "Oklahoma county", "Oklahoma", and "United States of America". To the left of the map, there is a list of referenced codes and standards, each with a link to "www.referencecodes.org/studied". The listed items include:

- Referenced by: IBC  
NFPA 101® Life Safety Code®  
Edition: 2015 [www.referencecodes.org/studied](#)
- Referenced by: IBC  
NFPA 105 Standard for Smoke Door Assemblies and Other Opening Protectives  
Edition: 2013 [www.referencecodes.org/studied](#)
- Referenced by: IBC  
NFPA 105 Standard for Smoke Door Assemblies and Other Opening Protectives  
Edition: 2013 [www.referencecodes.org/studied](#)
- Referenced by: IBC  
NFPA 221 Standard for High Challenge Fire Walls, Fire Walls, and Fire Barrier Walls  
Edition: 2015 [www.referencecodes.org/studied](#)
- Referenced by: IBC  
NFPA 221 Standard for High Challenge Fire Walls, Fire Walls, and Fire Barrier Walls  
Edition: 2015 [www.referencecodes.org/studied](#)
- Referenced by: IBC  
NFPA 252 Standard Methods of Fire Tests of Door Assemblies  
Edition: 2012 [www.referencecodes.org/studied](#)
- Referenced by: IBC  
NFPA 252 Standard Methods of Fire Tests of Door Assemblies  
Edition: 2012 [www.referencecodes.org/studied](#)

## Building Occupancy Codes

Next, establishing the [Building Occupancy Codes](#) will help define which portions of code apply to a given opening.

Occupancy codes impact which type of lock hardware can be fitted to doors, most commonly the use (or not) of exit devices and maglocks. In many cases 'one size does not fit all', and each opening can vary depending on the area's occupancy use classification.

In many cases these ratings are available in drawing sets or blueprints, usually labeled as an "Occupancy Schedule" like this example:

Occupancy Schedule										
Number	Name	Area	Non Calculate	Net Room Area	Area Per Occ	Occupancy Classification	Occup	Occup	Occupancy Load Equal Test	
100	RECEPTION	479 SF	0 SF	479 SF	15 SF	Assembly without fixed	32	32	Yes	
101	OPEN OFFICE	844 SF	0 SF	844 SF	100 SF	Business areas	9	9	Yes	
102	CORRIDOR	343 SF	0 SF	343 SF	0 SF	Unoccupied - Corridors,	0	0		
103	TRAINING ROOM	1028 SF	0 SF	1028 SF	7 SF	Assembly without fixed	147	147	Yes	
104	CONFERENCE	402 SF	0 SF	402 SF	15 SF	Assembly without fixed	27	27	Yes	
105	WORKROOM	428 SF	20 SF	408 SF	15 SF	Assembly without fixed	28	28	Yes	
106	STORAGE	384 SF	0 SF	384 SF	300 SF	Accessory storage area	2	3		
107	MEN	123 SF	0 SF	123 SF	0 SF	Unoccupied - Corridors,	0	0		
108	WOMEN	134 SF	0 SF	134 SF	0 SF	Unoccupied - Corridors,	0	0		
109	OFFICE	133 SF	0 SF	133 SF	100 SF	Business areas	2	2	Yes	
110	OFFICE	127 SF	0 SF	127 SF	100 SF	Business areas	2	2	Yes	
111	OFFICE	127 SF	0 SF	127 SF	100 SF	Business areas	2	2	Yes	
112	MECHANICAL	121 SF	0 SF	121 SF	300 SF	Accessory storage area	1	1	Yes	
Grand total							252	253		

Schedules indicate 'maximum loads' of people in specific room configurations, like 'standing room' or 'seated' capacities which often differ based on area and floor loading. Given the data like 'Occupancy Loads' and 'Occupancy (or Building) Classification', the proper codes for the space can be determined.

In other cases, the designer will need to [ask the AHJ](#) or perform calculations to be approved by the AHJ. We address the basic calculation method in the below section "Developing Manual Ratings".

## Establish If Opening is Emergency Egress

Finally, verifying if an access-controlled opening is an egress path can be confirmed by simple observation.

In many cases, if the opening is equipped by illuminated emergency exit signs, it is a positive indication the opening is a formal emergency egress door and not an internal entryway or corridor door.



Another option is to determine if subject doors are indicated on posted emergency evacuation plans:



The three criteria above will help access designers understand which codes impact system specifications.

### **Door Function Important**

Aside from building classifications, the function of a controlled opening is also an important consideration. The types of doors below have special considerations when installed as part of access systems:

- *Fire Doors*: The openings are more than just secured openings; they provide an integral safety function to limit risk in a fire condition. Because of this function, and their special construction, fire doors must be positively latched in a fire and cannot be cut or modified for hardware.
- *Stairwell Doors*: Usually stairwell doors are locked, to prevent unauthorized access during normal conditions, but in a fire these locks must be dropped so an occupant fleeing a fire cannot be trapped in a stairwell. For this reason, access-controlled stairwell doors are specially configured in typical use.
- *Delayed Egress Doors*: Other systems that momentarily 'lock inhabitants in' are subject to special authority, and the full scope of operation is typically governed by code, from how long a 'delay period' can be (15 or 30 seconds) or which doors can be kept closed to prevent unauthorized exit (i.e.: daycares and nursing home facilities).

Reconciling the security plan with the floorplan and facility occupancy code is vital, and clearly establishing what controls are permissible on which doors must be done upfront before any installation work commences.

## Building Occupancy Codes

A building or room's classification can greatly impact which building codes must be followed. In terms of access control, these 'occupancy codes' dictate how openings can be locked and what equipment is required, often representing a range of hundreds of dollars per door.



This instructs how to determine the occupancy classification of a space, and which codes apply.

The points we cover include:

- Why classification is necessary
- Code impact on lock hardware selection
- Classification definition and key categories
- Finding classification ratings
- Comparing classification types
- Handling mixed occupancies
- Developing manual ratings

## Impact On Access Control

Occupancy codes impact which type of lock hardware can be fitted to doors, most commonly the use (or not) of exit devices and maglocks.

Specifically, occupancy codes dictate where exit devices must be used to permit quick egress for most 'A', 'B', 'E', 'F', 'M', and 'U' groups. A residential 'R' classification does not require exit devices on doors.

In other cases, the local AHJ may restrict methods like [Delayed Egress](#) for certain occupancy codes only (ie: 'I' only) where the model codes do not restrict them at all. The same may apply to individual lock types like maglocks. The occupancy code may refine where or where not access control is allowed per local authorities.

The inclusion of exit devices on doors versus lever handles can greatly impact which type of electronic lock is used (e.g., mortise or surface strike) or even may exclude locks like maglocks from being legal to use.



For more on exit devices (shown above), see our [Exit Devices Tutorial](#).

In terms of the most common classifications, International Building Code (IBC) mandates Assembly 'A', Business 'B', or Educational 'E' occupancies, with an occupant load of 50 or more, require exit devices for doors equipped with a lock or latch. For any High Hazard 'H' occupancies, panic hardware is required regardless of the occupant load.

Another common codebook, NFPA 101 requires exit devices for doors serving Assembly, Educational, Business, and Day Care occupancies with an occupant load of 100 people or more. And finally, NFPA 70 (National Electrical Code) requires panic hardware or fire exit hardware on doors within 25 feet of the required working space for 'High-Voltage' areas, usually handling more than 600 volts, more than 800 amps, or battery charging/storage rooms for UPSEs or material handling lifts or forklifts.

### Why Classification Is Necessary

Unfortunately, a history of tragedies and deaths are the reason classification is needed.

The Winecoff Hotel Fire in 1946 is one example, where over 115 hotel occupants died because insufficient fire escape routes and egress had been designed into the building based on normal occupant loads. Other disasters like NYC's 1911 Triangle Shirtwaist Fire (shown below, killing nearly 150) also drove the importance of properly operated and designated egress routes in a structure, eventually resulting in forming the NFPA and modern life/safety codes as a direct consequence:



Modern occupancy codes are designed to make identifying critical protection areas easier, condensing egress requirements for even complex subsystems like physical access to a formula.

## Door Hardware Impacted By Code

For access, which type of door hardware is allowed or must be integrated with the system is often dictated by code. High-capacity occupancies often require special egress locks like [Exit Devices](#), and the occupancy code determines how mandatory they are to the area. We cover this deeper in the 'Impact on Access Control' section.

## Classifications Defined

While [building floorplans](#) and construction vary widely, the purpose of the buildings are similar and can be generally defined. Regardless of the appearance of the building, the gathering spaces, sleeping areas, factories, material storage, and commercial business activities it contains usually involve the same basic activities.

In terms of categorizing this, two major metrics are used, and from them an entire range of requirements are based. The need for multiple exits, fire escapes, sprinkler systems, ventilation, lighting, and even which type of door hardware can be used on doors is based on these categories:

- *Occupant Loads*: This rating determines the maximum number of people who can gather in a space simultaneously, depending on factors like area, available exits, building strength, and use type.
- *Building Classifications*: These ratings are concise, but general descriptions are given to a space based on how it is assigned for use.

Typically, both these ratings are calculated by architects or building engineers during design, but it is sometimes necessary for physical access control designers to figure these themselves.

## Ratings Found In Design Documents

In many cases these ratings are available in drawing sets or blueprints, usually labeled as an "Occupancy Schedule" like this example:

Occupancy Schedule									
Number	Name	Area	Non Calculate	Net Room Area	Area Per Occ	Occupancy Classification	Occup	Occup	Occupancy Load Equal Test
100	RECEPTION	479 SF	0 SF	479 SF	15 SF	Assembly without fixed	32	32	Yes
101	OPEN OFFICE	844 SF	0 SF	844 SF	100 SF	Business areas	9	9	Yes
102	CORRIDOR	343 SF	0 SF	343 SF	0 SF	Unoccupied - Corridors,	0	0	
103	TRAINING ROOM	1028 SF	0 SF	1028 SF	7 SF	Assembly without fixed	147	147	Yes
104	CONFERENCE	402 SF	0 SF	402 SF	15 SF	Assembly without fixed	27	27	Yes
105	WORKROOM	428 SF	20 SF	408 SF	15 SF	Assembly without fixed	28	28	Yes
106	STORAGE	384 SF	0 SF	384 SF	300 SF	Accessory storage area	2	3	No
107	MEN	123 SF	0 SF	123 SF	0 SF	Unoccupied - Corridors,	0	0	
108	WOMEN	134 SF	0 SF	134 SF	0 SF	Unoccupied - Corridors,	0	0	
109	OFFICE	133 SF	0 SF	133 SF	100 SF	Business areas	2	2	Yes
110	OFFICE	127 SF	0 SF	127 SF	100 SF	Business areas	2	2	Yes
111	OFFICE	127 SF	0 SF	127 SF	100 SF	Business areas	2	2	Yes
112	MECHANICAL	121 SF	0 SF	121 SF	300 SF	Accessory storage area	1	1	Yes
Grand total:					252		253		

Schedules indicate 'maximum loads' of people in specific room configurations, like 'standing room' or 'seated' capacities which often differ based on area and floor loading. Given the data like 'Occupancy Loads' and 'Occupancy (or Building) Classification', the proper codes for the space can be determined.

In other cases, the designer will need to [ask the AHJ](#) or perform calculations to be approved by the AHJ. We address the basic calculation method in the below section "Developing Manual Ratings".

## Classification Types

Here is a list of the occupancy classifications defined by the [International Building Code \(IBC\)](#):

1. Assembly: Groups A-1, A-2, A-3, A-4 and A-5
2. Business: Group B
3. Educational: Group E
4. Factory and Industrial: Groups F-1 and F-2
5. High Hazard: Groups H-1, H-2, H-3, H-4 and H-5
6. Institutional: Groups I-1, I-2, I-3 and I-4
7. Mercantile: Group M
8. Residential: Groups R-1, R-2, R-3 and R-4

9. Storage: Groups S-1 and S-2
10. Utility and Miscellaneous: Group U1

Rough classification is generally straightforward based on how the building or area is intended to be used. For example, houses are coded 'R', manufacturing plants coded 'F', and schools 'E'. From there, the sub-classification is based on specific use or size details further explained in IBC.

Take 'Factory and Industrial' codes F-1 or F-2. 'F-1' facilities carry a 'moderate hazard' rating, while 'F-2' means 'low-hazard'.

In the case of 'Institutional' or 'I' occupancies, the criteria I-1 is:

"[Area] houses more than 16 persons, on a 24 hour basis, who because of age, mental disability or other reasons, live in a supervised residential environment that provides personal care services. The occupants are capable of responding to an emergency situation without physical assistance from staff."

While I-3 is:

"[Area] inhabited by more than five persons who are under restraint or security and is occupied by persons who are generally incapable of self-preservation due to security measures not under the occupant's control."

So while the general use type is unchanged, the operational utility of the area has distinct definitions.

### **Mixed Occupancies**

Individual rooms or areas within buildings can be coded differently. This is an important feature in many buildings, and the exact classification of portions of a building can affect other critical variables like minimum fire protection equipment, number of elevators, emergency egress routes, or even lighting requirements for occupants.

In general, 'mixed occupancies' are a factor in access control because even if a small ancillary carries a more stringent life safety or egress requirement, it must be observed in any surrounding area.

For example, if a small 'high hazard' area is surrounded by a less stringent 'factory' rating, any egress paths must abide to the 'high hazard' classification. The same circumstance may apply on a floor of a college dormitory (perhaps an 'R' code) that contains a group study area or gameroom (an 'A' code). In that case, all common egress doors would need to be equipped with exit devices regardless if they were located in an 'R' area or not because of the 'A' mixed occupancy area.

### **Developing Manual Ratings**

If precalculated Occupancy Codes and Ratings cannot be found, the need may arise to do this manually. Occupancy Codes themselves are generally easy to determine, where the actual use type is compared to the criteria listed in Chapter 3 of IBC, titled "[Use and Occupancy Classifications](#)".

#### *Exit Availability*

In order to determine the maximum number of people who are able to safely be in a room or building, the IBC recommends a certain number of inches of doorway per occupant. Exits that adjoin a stairway need to have 0.3" of doorway per person, and all other exits need 0.2" of doorway per person.

Take an example meeting room hall that has a maximum occupancy of 500 people. That room needs at least 100" - 150" of doorway. With doorways at around 36 inches in width that function hall would need approximately three to five doors.

### *Occupant Load*

To calculate the occupant load, the first step is to calculate the area of the space in question by multiplying the length times the width along the floor. For example, if a boardroom measures 40 feet (~12m) by 50 feet (~15m), the room area measures 2000 square feet (~609 sq. m). The next step is to divide that figure by the occupant load factor found in IBC(2012) [Table 1004.1.2 – Maximum Floor Area Allowances per Occupant](#), which varies depending on the Occupancy Code. The resulting value provides how much floor per occupant is allowed.

Once the manual occupant load has been calculated, it can be used as guidance against whether or not Exit Devices must be used/kept on doors, or whether or not the AHJ's local exception rules like 'No Maglocks' apply to the space.

[Note: this was originally published in 2016 and substantially rewriteen in 2018.]

# Free Online NFPA and IBC Codes and Standards

Finding applicable codes for security work can be a costly task, with printed books and pdf downloads costing hundreds or thousands. However, a number of widely referenced codes are available free online if you know the right places to search.

This post provides link to a number of free code resources common to security including:

- NFPA 70
- NFPA 72
- NFPA 80
- NFPA 101
- International Building Codes (IBC)

## NFPA Online Free

The NFPA provides the standards used as code basis for multiple aspects of security integration, including the National Electrical Code, authoritative Life-Safety guidelines for access control, and multiple related standards for Fire Alarms, Firewalls, and Fire Doors.

The NFPA provides [free online reference access to all ther latest versions of all standards](#) after free registration is completed. The most relevant NFPA standards used in security include:

### **NFPA 70: NEC, The National Electrical Code**

In most of North America, the most comprehensive guide is NFPA 70, most commonly called the 'NEC' or National Electrical Code. While the scope of the codes mainly apply to high-voltage electrical work of more than 100 Volts, security work and devices like PoE or small gauge cabled hardware using less voltage are also given prime attention.

- [NFPA 70: National Electrical Code](#) (registration required)

## NFPA 101: Life Safety

One of the most important guidelines of electronic access is NFPA 101, the foundation behind how to install access and still preserve safe egress. We examine those elements closely in our [Codes Behind Access Control](#) post, but free access is available here:

- [NFPA 101: Life Safety Code](#) (registration required)

## NFPA 80: Fire Door Modifications

Because fire doors have important functions to prevent the spread of fire and to withstand direct flames for some time, modifying them for electronic access use is limited. In most cases, NFPA 80 describes the extent and size of cutouts or holes allowed in a fire door, or the acceptable behavior of that hardware given the location of the door. The link below offers direct access to the section:

- [NFPA 80: Standard for Fire Doors and Other Opening Protectives](#) (registration required)

## International Building Code

Taking central importance in legal building design, and retrofit systems like access, IBC is often cited by local jurisdictions as the authority on how to construct systems safely. As we cover in [Building Occupancy Codes and Access Control Tutorial](#) and our [Codes Behind Access Control](#) notes, the actual version that is adopted can vary by year, with verbiage and citations change between them. Below are the most common versions cited today:

- International Building Code 2015 [link no longer available]
- International Building Code 2012 [link no longer available]
- International Building Code 2009 [link no longer available]

## **Fair Use Copyright Applies Here**

In general, free online code resources are read-only and users are not able to download, notate, or print copies for offline circulation. If users want this, then standards and codes are available for purchase, often at prices ranging from ~\$100 for a single standard to upwards of \$5000 for a full set of comprehensive codes. For example, NFPA explains:

"These online documents are "read-only" - they cannot be downloaded or printed, because NFPA relies on the revenues from individuals who [purchase copies of these documents](#) to fund our mission. But these "read only" documents are available to anyone who wants to familiarize themselves with a code or check a requirement."

Under terms of 'Fair Use', citation and republishing of excerpts for public commentary or criticism is allowed, but wholesale republishing of the codes or standards can only be done under conditions given by the authoring agency.

[Note: This guide was originally written in 2016, but substantially updated in 2018.]

# Access Control ADA and Disability Laws

Safe access control is paramount, especially for those with disabilities.



Most countries have codes to mandate safe building access for those who may have difficulty with 'traditional' building design. In the US, the "[Americans with Disabilities Act \(ADA\)](#)" are these codes, while similar requirements are found in [Canada's Bill C-81](#) and the [UK's 2010 Equality Act](#).

We examine the most common ways disability and accessibility codes impact access control design.

## Key Access Control Requirements

The top 3 ways accessibility codes impact access control design are:

1. Door Hardware Must Be Compliant
2. Turnstiles Must Include Gates
3. Accessible Reader Height/Door Controls

Other potential impacts related to delayed egress, door operators, mantrap/breezeway design, and double door configurations, but those elements are seldom constructed in a way needing changes due to access control modifications.

Typically when corrective action is needed, it occurs because of other construction impacts openings or due to the end of previously grandfathered exemptions ending.

## International Accessibility Rules

While ADA is US legislation, it is used as a guideline internationally. Many countries have their own rules, but the scope and many regulations are patterned after ADA.

For a directory of individual country regulations, [see the UN's list by member country](#). While not all countries enforce the guidelines as laws like the US, many have adopted accessibility codes as 'best practices' and they should be followed where possible.

In recent years, the United Nations has accepted ADA and general guidance international accessibility guidelines that have been ratified or principally accepted by several countries:



## **Canada and UK Rules**

In general, the requirements of Canada and the United Kingdom generally match the ADA, (although the ADA often is more explicit). Especially in Canada, local provisional/municipal jurisdictions may enforce more strict rules, like [Vancouver's Doorknob Ban in Private Homes.](#)

For Canada and the United Kingdom, the applicable basis for building and accessibility rules are:

- [Canada With Disabilities Act \(Bill C-81\)](#)
- [UK Equality Act of 2010](#)

## **US Mandate For Public, Commercial, but not Residential Buildings**

The Americans with Disabilities Act was signed into US law in 1990 and most recently [amended in 2010.](#)

In general terms, [28 CFR Part 36](#) addresses building structural and subsystem design, ensuring that anyone with a 'disability' - wheelchair, blindness, hearing, or "*any physical or mental impairment that substantially limits a major life activity*" has equal access to, within, and from a commercial or public building.

ADA does not apply to private dwellings, 'historically significant' structures, or other specifically exempted buildings.

Nor does it apply to 'new construction' only. In fact, the most dramatic aspect of ADA is its applicability to existing buildings. The law spells out that aspect here:

### **4.1.6 Accessible Buildings: Alterations.**

**(b) If existing elements, spaces, or common areas are altered, then each such altered element, space, feature, or area shall comply with the applicable provisions of 4.1.1 to 4.1.3 Minimum Requirements**

In plain terms, existing buildings are often allowed to remain in a 'non-compliant' state until audits or improvements force the update. In many situations, adding or upgrading access control systems qualify as a 'improvement', and so the move to compliance must be taken as a result.

## Door Knobs and Many Handles Are Not Allowed

One subtle, but potentially costly change is the prohibition of rounded knobs on door hardware sets. The code excerpt forbidding knobs is shown at right:

**4.13.9\* Door Hardware.** Handles, pulls, latches, locks, and other operating devices on accessible doors shall have a shape that is easy to grasp with one hand and does not require tight grasping, tight pinching, or twisting of the wrist to operate. Lever-operated mechanisms, push-type mechanisms, and U-shaped handles are acceptable designs. When sliding doors are fully open, operating hardware shall be exposed and usable from both sides. *Hardware required for accessible door passage shall be mounted no higher than 48 in (1220 mm) above finished floor.*

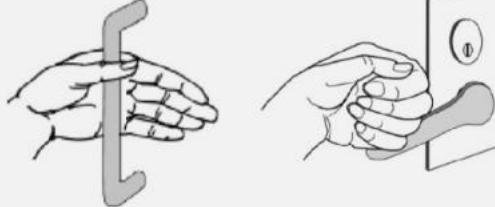
Specifically, the law emphasizes that door hardware have 'lever-style' handles, where rotating the lever retracts the latch.

With the number of options available, it is possible to specify illegal types:



Especially with 'stand-alone' access control locks, paying attention to the trim handle specification means making more than a cosmetic decision.

Auditing and replacing all access controlled door handles with lever or open handles/exit devices is required to be compliant:

**ADA ACCESSIBLE DOOR HANDLES****Turnstiles must have Gates**

Likewise, when it comes to turnstiles or revolving doors, an adjacent gate or hinged door must be installed that permits those in wheelchairs passage through the opening:

**4.13.2 Revolving Doors and Turnstiles.**  
Revolving doors or turnstiles shall not be the only means of passage at an accessible entrance or along an accessible route. *An accessible gate or door shall be provided adjacent to the turnstile or revolving door and shall be so designed as to facilitate the same use pattern.*

In many cases, the gate is a separate entry/egress path from the turnstile, and can increase required opening areas by more than double:

**Wheelchair Access Through Turnstiles IPVM**

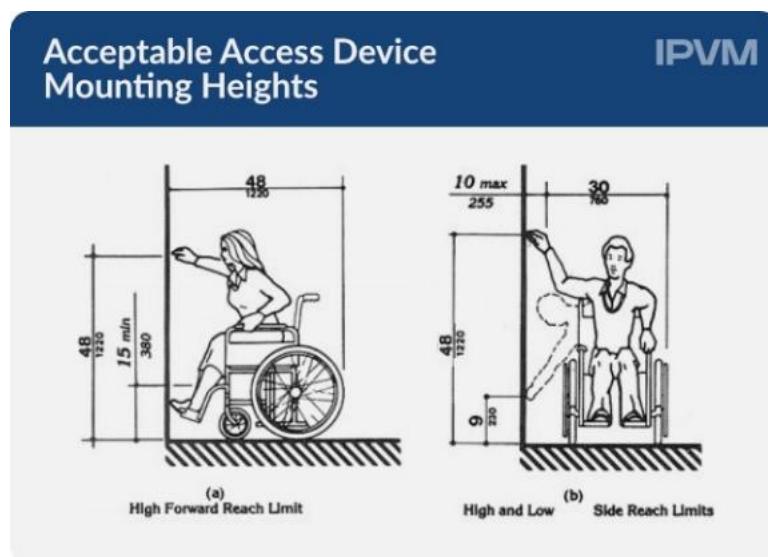
A common concern with 'ADA Gates' is that they simply become 'another opening' to be used by all occupants and become opportunities for [tailgaters to 'sneak in'](#) to a facility.

For this reason, many access systems [grant special access permissions](#) to those in wheelchairs so that only they are able to open the gate. Otherwise, all other occupants can only travel through the turnstile or revolving door.

### Accessible Reader Height/Door Controls

All access control user interfaces like readers and intercoms must be within reach of those in wheelchairs.

This limits the mounting height to no more than 48" above the floor, regardless if the reader is mounted in front or to the side of the door:



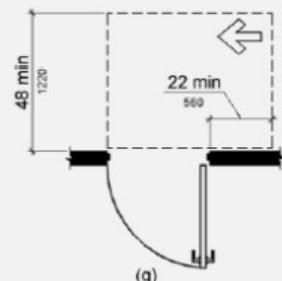
This standard also applies to other door control equipment, like [RTE buttons](#) and powered opener switches.

The clearance for door swings and the time a door is unlocked may also be increased on these openings, to allow for the extra time needed to reposition the chair and roll through the opening.

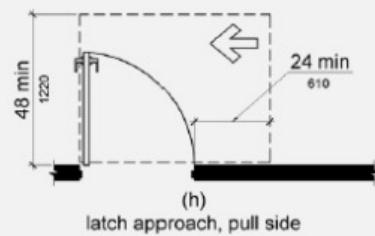
The exact dimensions and locations of required clearances vary according to the type and [swing of the door](#):

## Clearances Specific To Door Type

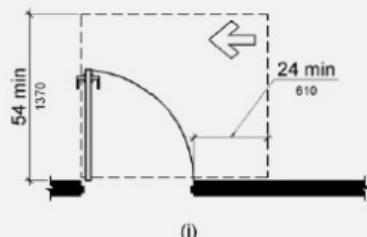
IPVM



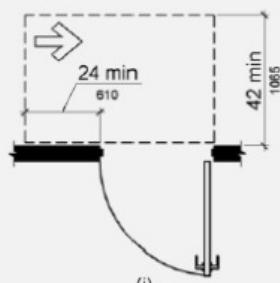
(g)  
hinge approach, push side, door  
provided with both closer and latch



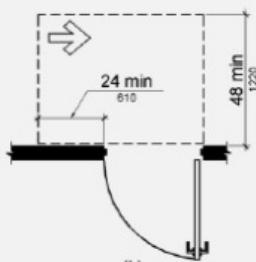
(h)  
latch approach, pull side



(i)  
latch approach, pull side,  
door provided with closer



(j)  
latch approach, push side



(k)  
latch approach, push side,  
door provided with closer

# Standard for Access Control (UL 294)

Few specifications are seen more commonly in access control than UL 294. However, aside from seeing it in print, very few understand what it means. In this note, we break apart and define this spec, describing why it is a vital part of many Access RFPs.

## A Standard Defined

The scope of UL 294 [link no longer available] covers three aspects of Access Control systems:

- Construction (Installation)
- Performance
- Operation

Essentially, the heart of UL 294 is a safety standard, where testing proves that system components can be assembled and operate reliably without hazard. In the case of access control, this is a step beyond just validating devices will not catch fire or spark - it attests that the system will not harm the safety or impede egress of those using the system.

In practical terms, this means doors will not accidentally stay locked and keep people in harm's way even during a malfunction. The UL standard subjects each labeled device to a range of testing designed to show the equipment meet relevant code expectations from:

- *NEC (NFPA 99)*: Requirements that each component will not create a hazard either during (recommended) install or use (Sparking, Grounding)
- *NFPA 72*: Fire Code compliance, assures that controllers include interfaces with fire alarm/suppression systems
- *NFPA 101*: System devices

A UL 294 mark is a 'extra step' the vendor has taken to 'prove' their equipment is safe, and it stands as a 'mark of assurance' when included in buying specifications that dubious equipment will not be purchased.

## The Mark

While Underwriter's Laboratories [offer a range of 'UL Symbols'](#) that can be interpreted to signify different standards. In the case of UL 294, the mark looks like this:



The UL 'Security Mark' applies only to products such as intrusion detectors, burglar alarms, access control, safes, and vaults.

## Performance Tests

UL 294 includes several tests that evaluate how well devices withstand damaging environments. Devices are subjected to atypical electrical, environmental, and brute force situations, including:

- Variable Voltage
- Variable Ambients (Environment)
- Humidity
- Endurance (Ruggedness)
- Transients
- Corrosion
- Standby Power (Battery backup)
- Physical Attack Toughness

Tests are performed individually and are not 'layered' or 'stacked' simultaneously as might occur in the field. The exact methodology for each test depends on the device being tested, but the resulting grade is given in four levels of security performance with Level I (lowest level security equipment) to Level IV (highest level security equipment).

## **Exclusions**

However, not all parts and features of an Access platform fall under the scope of UL 294. Two areas excluded from the scope include:

- *Headend Server/Database*: The scope reads "The accuracy of logged data is not evaluated by this standard", and also "This standard does not apply to supplementary computer equipment that is not necessary for operation of the access control system..."
- *Intrusion Detection*: Again, the scope details "Where an access control equipment and/or system incorporates the features and functions of a burglar alarm control unit, the requirements of the Standard for Proprietary Burglar Alarm Units and Systems, UL 1076, shall also apply"

This is important to note when careless specs are written that "All Access Equipment shall be UL 294 Certified", because this is inherently not possible. There will be major functional aspects outside the scope of the standard.

## **Large System Adoption**

Especially for larger systems, UL 294 is common, including devices from: Mercury Security [link no longer available], [C\\*Cure](#), S2 [link no longer available], Maxxess [link no longer available], Sargent [link no longer available], etc.

However, certification is done on a component basis, and there may be gaps in a brand's portfolio. If UL 294 compliance is required in a system, every hardware component must be checked for conformity, as there is no 'system' certification.

Systems and platform intended for smaller deployments (<100 doors) typically forego the certification, because it simply is not a purchasing driver for many non-enterprise customers.

## **Prime Use**

Regardless of the 'safety' overtures, like [UL certification for surveillance equipment](#), 294 is primarily used to exclude non-compliant systems from specifications. UL 294 evaluation is not mandatory for Access Equipment, and many vendors forego the cost of certification especially when their offerings are not well suited for larger government, institutional, and hospital verticals where 294 is commonly cited.

Likewise, while the mark's testing 'proves' that devices are safe, the onus remains on the field technician to install them in the correct fashion to indeed live up to the certification.

## **Fail Safe vs. Fail Secure**

Few terms carry greater importance in access control than 'fail safe' and 'fail secure'.



Access control professionals must know how these concepts apply, and how to select locks that are appropriate.

We teach:

- The difference between 'fail safe' and 'fail secure' locks
- Why free egress is important
- Controlling entry is the goal
- Mechanical overrides for fail secure
- When to use fail secure hardware
- Typical access locks for fail safe and fail secure
- Proper application of maglocks and strikes for 'fail safe' and 'fail secure'

Finally, after reading, [take our 5 question quiz](#).

## Terms Defined

These terms have a specific meaning for door hardware. Whenever these functions are cited in specifications or code passages, they mean:

- Fail safe: When power is interrupted (fails), the electronic locking device is released (unlocked).
- Fail secure: When power is interrupted (fails), the electronic locking device is secured (locked).

These behaviors can impact hardware design and access control configuration, so noting the situations where each is used is very important.

## Free Egress ALWAYS

One misconception of these terms surround which side of the door they apply.

'Fail secure' and 'Fail safe' terminology generally applies to ENTRY control only, meaning manual egress in most [Building Occupancy Codes](#) is allowed at all times. In an emergency situation, nothing should impede egress (or exit) from a building.



Just like locking or chaining exit doors have resulted in terrible tragedies, a significant majority of life-safety authorities simply will not allow locks to complicate exiting.

This means that exit doors must always be equipped with mechanical means to override electrified locks (i.e.: [panic bars or exit devices](#)) and if electrified hardware cannot be made to 'fail safe', it cannot be used.

### 'Fail Safe' Typically Required, With 'Fail Secure' Exceptions

In most cases, door locks are required to 'fail safe'.

However in specific applications, 'fail secure' is required by code. The most common areas where this is the case:

- *Fire Doors:* These doors provide structural barriers to the spread of flame during a building fire, and are common features of fire control design, where a closed-door is used to seal off a portion of an engulfed structure. It is critically important for a fire door to remain closed in a fire, and positive latching 'fail secure' hardware is often specified to ensure a positive lock is always the case regardless of power.
- *Stairwell Doors:* In many building occupancies, all stairwells are locked to reentry from the outside, so that evacuation always leads outside and not potentially into harm inside. This remains one of the most modified and scrutinized pieces of code, with many code revisions over the years resulting in confusion among AHJs.

Less common occupancies, like jails, prisons, mental health care facilities, or nursing homes may use Fail Secure almost exclusively but are typically heavily regulated and other methods of safe emergency egress are often required.

## Controlling Entry is the Issue

Firedoors Require Fail Secure IPVM

However, 'fail safe' vs. 'fail secure' is a critical aspect of managing entry into a building during an emergency.

Firefighters or medical responders could be locked out of an area if it is not properly configured to 'fail safe'. On the other hand, occupants could inadvertently open a fire door, exposing otherwise protected parts of a building if 'fail secure' is not properly implemented.



The behavior of hardware when power drops is a key part of building design, and both functions play a key role in safely entering a potentially enveloped facility.

## Mechanical Overrides

Where 'fail secure' hardware is used, local [AHJs](#) often require a mechanical override. In the case of strikes, the existing lever lock or exit device provides this function, but other types of electrified hardware may require additional 'mechanical key override' components.

For example, in the image below the exit device always allows free egress from the inside, but a keyed latch allows outside access even if the strike or electronic latch 'fails secure':



However, the mechanical override is also a source of trouble in many access controlled doors. If someone gains entry using a key, access is granted without the 'system' able to log who entered. Unless [key control](#) is tightly implemented, mechanical overrides result in 'door forced' errors in access control logs, and bypass system recording individual access.

As a result, the use of Mechanical Override Keys is often used only on an emergency basis with relatively few keyholders - by nature, these operational restrictions are often too complex for many end-users to adopt.

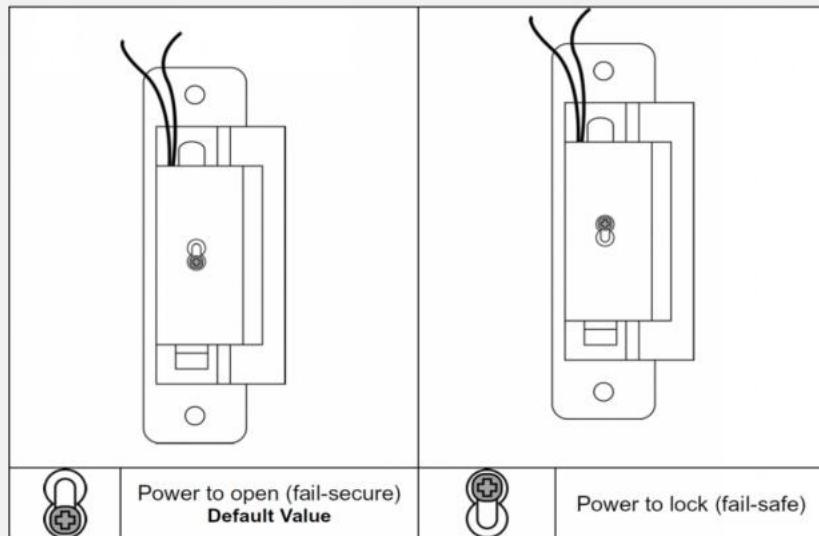
### **Field Configurable Locks**

Some electronic access locks can be made to behave either 'fail safe' or 'fail secure'.

The most common example are [strikes](#), where commonly the position of screws or dipswitches change how the lock functions when power fails:

## Example Field Configured Strike

IPVM



### Designing Default Fail Safe Eliminates Risks

For most openings, the default function is to 'fail safe', unless otherwise noted on design documents, hardware schedules (see image below), or other engineering plans as 'fail secure required'.

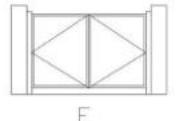
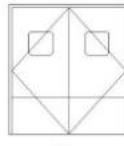
The exact verbiage of this instruction will vary according to the source, but since adoption of 'fail secure' locks is limited, they are nearly always called out in an excepting or special manner:

# Example Blueprint Door Schedule

IPVM

HARDWARE SCHEDULE	
HARDWARE #1	HARDWARE #2
THRESHOLD POMKO #2548D	THRESHOLD POMKO #2548D
HINGES POMKO NO. FM89HD (1 1/2 PAIR)	HINGES STANLEY #FB8199 (1 1/2 PAIR)
CLOSER CORBIN-RUSSELL	CLOSER LCN #1460
PUSH PLATE BUILDERS BRASS WORKS	LOCK-SET SCHLAGE D-SERIES
LOCKSET #	LEVER TEE
LOCKSET BUILDERS BRASS WORKS	LOCK PANIC HARDWARE
LOCK #5025-630/530	BEST #1C-7-A-C49P3-62B
LOCK PANIC HARWARE	DOUBLE KEY HOLE
BLIND PLATE #4-C49P3-626	KICKPLATE BUILDERS BRASS WORKS
DOUBLE KEY HOLE	ALUMINUM KICK PLATE
KICKPLATE NONE	MISC WEATHERSTRIPPING DOOR SNEEP
MISC	
WEATHERSTRIPPING DOOR SNEEP	
HARDWARE #3	HARDWARE #4
THRESHOLD NONE	THRESHOLD POMKO #2548D
HINGES STANLEY #FB8199 (1 1/2 PAIR)	HINGES STANLEY #FB8199 (1 1/2 PAIR)
CLOSER LCN #1460	CLOSER LCN #1460
LOCKSET NONE	LOCK-SET SCHLAGE D-SERIES
PUSH PLATE BUILDERS BRASS WORKS	LEVER TEE
LOCKSET #	LOCK PANIC HARDWARE
LOCKSET BUILDERS BRASS WORKS	BEST #1C-7-A-C49P3-62B
ALUMINUM KICK PLATE	DOUBLE KEY HOLE
SYMBOL OF ACCESSIBILITY	KICKPLATE BUILDERS BRASS WORKS
	ALUMINUM KICK PLATE
	MISC DOOR STOP

DOOR SCHEDULE						
DOOR NO.	DOOR TYPE	SIZE	MAT.	FINISH	HRDWR	REMARKS
1	A	3'-0"x7'-0"	WOOD	P-1	1	PANIC HARDWARE ON THE INSIDE
2	A	3'-0"x7'-0"	WOOD	P-1	1	PANIC HARDWARE ON THE INSIDE
3	C	3'-0"x7'-0"	STEEL	*	2	NO LOCK FROM THE OUTSIDE * FINISH SHALL MATCH EXTERIOR FINISH
4	C	3'-0"x7'-0"	STEEL	*	2	NO LOCK FROM THE OUTSIDE * FINISH SHALL MATCH EXTERIOR FINISH
5	F	3'-0"x7'-0"	WOOD	P-1		
6	E	6'-0"x8'-0"	STEEL	*		NO LOCK FROM THE OUTSIDE * FINISH SHALL MATCH EXTERIOR FINISH
7	E	6'-0"x8'-0"	STEEL	*		MANUFAC. * FINISH SHALL MATCH EXTERIOR FINISH
8	B	3'-0"x7'-0"	WOOD	P-1	3	PANIC HARDWARE
9	D	3'-0"x7'-0"	POLYMER	MANUFAC.	MANUFAC.	ELUSON DOOR #SCP-11 OR APPROVED EQUAL
10	F	3'-0"x7'-0"	WOOD	P-1	4	
11	F	3'-0"x7'-0"	WOOD	P-1	4	LOCKABLE FROM INSIDE
12	A	2'-0"x7'-0"	WOOD	P-1	1	
13	F	3'-0"x7'-0"	WOOD	P-1	1	LOCKABLE FROM INSIDE



## Maglocks Are 'Fail Safe'

By design, [maglocks](#) require electricity to operate, so when power is removed they 'fail safe' by default. The drop in power is often a condition of the fire alarm system so that if any fire pull is activated, all maglocks drop power at the same time. This can cause issues with building security, as then [link no longer available]certain exterior doors are unlocked and able to be accessed from the outside, so mechanical locks are an important feature in many of these doors.

Supplying backup power to maglocks is not widely adopted for most openings. When backup power is used with maglocks, it must happen with the concurrent blessing of the AHJ and still be installed so power fails during an emergency event. See our: [How To Use Maglocks With Battery Power Legally](#) note for guidelines.

## But Strikes Often 'Fail Secure'

These devices can commonly be field configured for either 'fail safe' or 'fail secure' function.

Our [Selecting the Right Electric Strike](#) guide covers low-level operation, but since most 'keeper' elements of strikes are driven by solenoids, changing the default polarity of the solenoid can cause the keeper to be rigid on loss of power, or completely moveable.

Since the configuration of either function is typically a simple setting, strikes are often the favored devices to provide 'fail secure' functionality. Since the mechanical hardware on the door already permits mechanical egress, strikes are simple additions to the controlled opening to provide this feature.

*Other Hardware:* There are a number of other 'fail secure' hardware devices available, including electronic deadbolts, keypad locks, and electrified locks. However, the adoption and use of this hardware may not comply with codes relating to emergency egress paths and are not commonly used in fail secure configuration. [link no longer available]

## Quiz

Finally, after reading, [take our 5 question quiz](#).

## AHJ / Authority Having Jurisdiction

One of the most powerful yet often underappreciated characters in all physical security is the Authority Having Jurisdiction (AHJ).



Often, these authorities get involved only when problems arise, and they frequently leave a flood of delays, redesigns, and cost increases in their wake.

We examine:

- Who AHJs Are
- What Job Titles They Typically Hold
- What Qualifications They Have
- Why Video Surveillance Does Not Typically Concern AHJs
- But Why Access Control Systems Typically Do
- Why Initiating Contact With AHJs Is Prudent

This tutorial will help security installers improve their AHJ interactions in security projects.

## AHJs Defined

'Authority Having Jurisdiction' is an official designation used in many organizations, including governments, military, construction, and a variety of trades. The term identifies specific people or organizations responsible for ensuring all work is compliant.



The realm of 'compliance' varies according to who the authority represented. For access control, the AHJ is most often interested in confirming the system will not endanger life safety during an emergency.

However, AHJs often represent other interests security installers do not typically consider - the cosmetic appearance of the equipment, modification of landscape (ie: trimming trees), and if the security system somehow interferes with another building system.

Because individual 'jurisdictions' vary, the actual job titles of AHJs are diverse. However, without exception, AHJs represent the interests of overarching regulations, codes, or local influence. When AHJ direction is not recognized or ignored, the problems impacting projects can quickly drive costs and delays, as several members note in [Access Control AHJ Nightmares](#).

## Who Are They?

The AHJs often change depending on the type of work you are performing, but for most intrusion alarm and access control work, they are found in two prime authorities:

*Fire Marshals:* Also called the 'Fire Inspector', this office is tasked with enforcing fire codes. The scope of enforcement includes field surveys of installation work, and may even mandate project plan signature approval.

***Building Inspectors:*** This authority ensures that all work is performed within the constraints of written building codes. Not only are they versed with interpreting national codes, but they know the local exceptions and addenda.

Other less common, but potentially influential, organizations that have AHJs are found in:

- Health Departments
- Engineers/Architects
- Senior Executives
- Utility Companies
- Military Installation Commanders
- Insurance Companies

In general, the best method of identifying the AHJs for a project is to start by asking the owner's representative and the local Fire Chief for contact names in the area of your work. The type of answer you receive will often lead to expectations of how strict or complex the tiers of authorities are for an area. In some areas, there might be a single AHJ to get approval from, while there may be a disjointed litany of AHJs in other areas.

Regardless, knowing who these individuals are, and the prerogative they are checking your work from, becomes an invaluable part of getting your job done right, on time, and within budget.

### **Why AHJs Matter**

Right or wrong, AHJs play a huge role in the outcome of security projects. Few individuals are given authority to stop work based on their decisions, but AHJs wield this authority daily.

Where does this authority come from, and why do they have it?

- *They are Educated:* While they may not be technical experts on alarm system or door access control design, AHJs have extensive knowledge on specific codes or regulations

that constrain security work. They seldom will express a pure opinion, but instead, cite specific code passages or laws when objecting to a work element.

- *They are Experienced:* AHJs are often elevated to their positions after years of ground-floor, in-the-trenches experience. When they do share a strong opinion, it is frequently tempered by 'having seen it before'. Most AHJs take the lessons learned from other similar projects and apply them forward.
- *All the Risk, None of the Reward:* Often, it is not a matter of agreeing or disagreeing with their views, because their determination is final. They are bound to their decisions by oaths, laws, and general liabilities. When a system is safe or compliant, an AHJ 'wins' by going unmentioned, and only when a disaster occurs will many AHJs even be recognized.

## AHJs In Video Surveillance

While important to security operations, many video surveillance systems fall outside the oversight of AHJs. Because video does not determine or impact Life Safety for facilities, its use is not subject to the same regulations as fire alarms and access control systems.

Usually, if AHJs are involved in video, it is to confirm the UL conformance of devices and install methods so that building certifications are not invalidated. The applicable UL ratings vary, but common ones for video are:

- [UL Standard 60950](#): Is the most common for cameras, and applies to low voltage safety (ie: non-combustibility)
- [UL Standard 2043](#): Applies when plenum mounting low voltage equipment

## AHJs In Access Control

However, the involvement, interest, and concern for access systems is a big concern. Given that access can cause injury, harm, and even death to building occupants if installed improperly, AHJs typically consider their approvals and inspection of the systems a core responsibility.

As addressed in our [Building Occupancy Codes and Access Control Tutorial](#), [The Codes Behind Access Control](#), and [Disability Laws, ADA and Access Control](#) notes, the role of the AHJ is distilling code compliance often requires involved and prolonged access project participation.

## Practical Examples

Our experience as integrators has turned up a variety of AHJs specific to particular jobs, including:

- *Fire Chief*: Most cities yield life/safety determinations to the local fire marshal, who in some cases might also be the top-ranking local fireman or the 'Fire Chief'. The issue of '[Fail-Safe vs. Fail-Secure](#)' is foremost to many of these firefighters.
- *Flightline Officer in Charge*: For many airports, the flight line is the hub of activity, and any equipment that impacts flight operations is significant. For example, USAF bases often have a hard restriction on a piece of equipment installed higher than 8', because it could interfere with aircraft movement on the flight line.
- *Director of Maintenance*: These entrusted individuals know relevant codes in a facility. Getting 'buy-off' from the head of maintenance often puts others at ease, knowing the 'local AHJ' approves.
- *Arsenal Commander*: For a munitions storage facility, any activity involving the running of electricity (regardless of voltage) required explicit approval from the commander, who required a defined work plan of equipment review, laborer background checks, and safety briefings before permitting work.
- *Municipal Codes Inspector*: Like the Fire Chief, the code inspector often acquires responsibility of signing off on installed systems as part of their job. Knowing the local inspector, and sharing code interpretation in the course of normal communication can yield trust and understanding during the course of many installations.

## Take the First Step

The best approach to working with AHJs is to be the first to reach out for approval.

AHJs are frequently challenged by the volume of work they should be monitoring, and they are not always patient or understanding when they are indirectly informed of your project.

In the attitude of 'asking for permission, rather than forgiveness', security designers and installers can win the cooperation of an AHJ before commencing work, rather than skirting the matter and being 'caught' later.

Not only will the basis of the relationship be 'proactive' rather than 'reactive', but the AHJ can also offer information or contacts that benefit the installer in future efforts.

[Note: This post was substantially revised in 2020 after its original publication in 2013.]

# Doors & Locks

## Door Fundamentals

Doors vary greatly in how difficult and costly it is to add electronic access control. Bad assumptions about them can cost thousands.



Often the door is inadequately or inaccurately described resulting in avoidable specification mistakes. In this note, we examine how to properly identify a type of opening using industry terms:

- Leafs
- Mullions
- Frames
- Lites and Transoms
- Door Swing

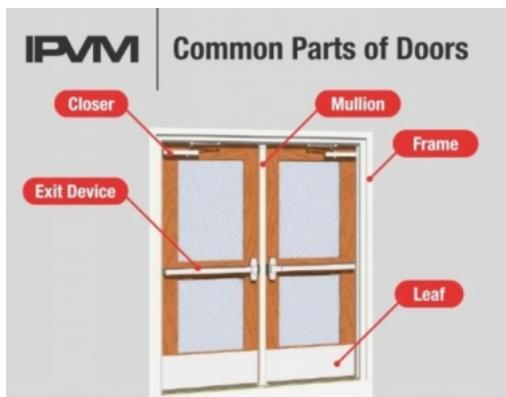
And we examine common door types often used in access control:

- Steel, Wood, and Glass Doors
- Automatic Sliding Doors
- Rollup Overhead Doors
- Reading Door/Hardware Schedules

## Common Door Components

While door sizes, shapes, and appearance may vary, commercial door openings typically contain the same features, elements, and pieces.

Basic door anatomy looks like this:



Below sections clarify individual elements called out above.

### Leafs

The 'leaf' is the main swinging part of a door. A single door is often called a 'leaf', while a double-doored opening has two 'leaves'. On double doors, sometimes one of the 'leaves' is held stationary and is locked in place, while the other swings freely. This is typically called the 'active leaf'.

### Mullions

Sometimes 'leaves' are separated by a bar stop running vertically between them called a 'mullion'. Mullions can be permanently affixed as part of the frame assembly or may be a removable type, which are typically locked into place to prevent unauthorized removal (and threaten the security of the opening).

The mullion often plays a key role in securing the door, because it contains the cutouts that the companion door locks physically extend latches into. When mullions are not part of a double

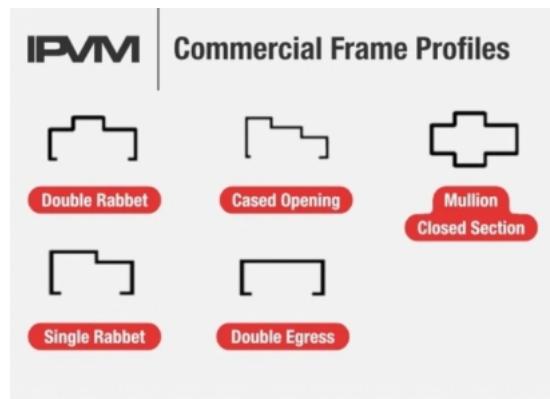
leaf opening, vertical rods that secure door latches into the top or bottom edges of a door are used.

## Frames

Key elements of "Frames" include material used and its 'profile':

- Steel and Aluminum are common materials used to construct frames, although wooden frames can sometimes be found on older buildings.
- The 'profile' of the frame - or the shape in which it constructed is often dependent on aspects like the adjacent wall to which it is attached, the type of door it is intended to frame, the swing of that door, and the type of hinges it is designed to work with.

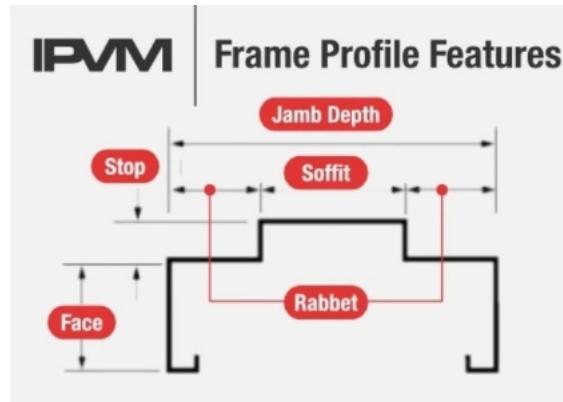
The image below is an example of the most basic frame profiles used in commercial openings:



The frame profile can impact the type of lock used to secure the door, especially if the frame profile does not permit enough clearance to recess or embed the lock within the frame, as is common with [Electric Strikes](#).

Most commercial doors use a 'double rabbet' frame profile, although most buildings also use 'single rabbet' and 'double egress' frames sporadically.

Here is a closer look at standard frame profile features and the way they are identified in lock mounting instructions:



The shape and dimensions of a frame, especially the 'face' depth, can impact how much space for access control devices like [strikes](#) and [door position switches](#) are available, or how cabling is run to devices like readers. When specifying electronic strikes or hanging readers from frames, make sure that enough room for the device and the device wiring exists inside the frame.

## Exit Devices

Also called 'panic bars' or 'crash bars', these components allow the door to be swung open by pushing on the mechanical latch bar. This type of lock is one of the most common door elements to interface with access control, and their use is often mandatory per [Building Occupancy Codes](#).

For more, see our [Exit Devices For Access Control Tutorial](#) that gives an in-depth look at the component.

## Lites and Transoms

'Lites' and 'transoms' refer to the pieces of glass within or adjacent to the door leaf itself. It is a common feature to have a full-height glass sidelight adjoining an entry door. These features are important to note due to the impacts they may provide access control features like wire runs or the mounting options of items like maglocks.

Here's an example:



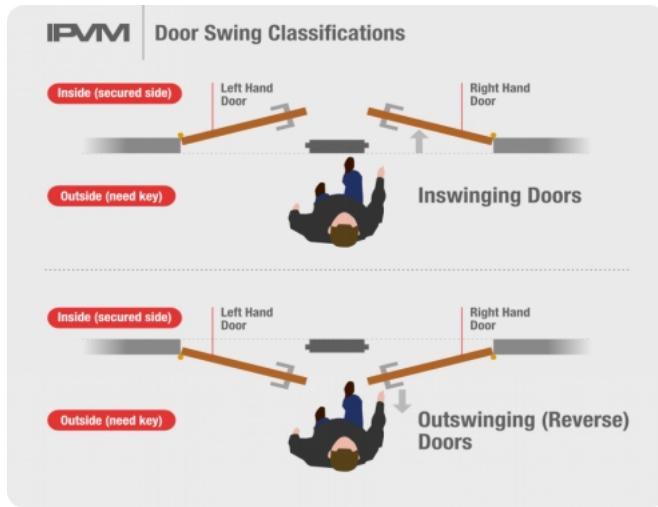
## Door Swing

The direction a door swings can greatly impact door hardware selection. There are four basic ways a door can swing, and knowing how to properly describe it is critical when designing access control systems and ordering door hardware.

Openings are configured to have doors swing in four separate ways:

- *Right Hand*
- *Left Hand*
- *Right Hand Reverse*
- *Left Hand Reverse*

The differences in these types are best described with diagrams. The images below show all four types:



Especially when using maglocks, not noting door swing can be a costly mistake either due to improper installation or a security risk due to exposed power cables. For more, see our [Door Swing Tutorial](#) post.

## Type of Doors

In general, care must be taken to understand the construction of the door and any special ratings it may possess (ie UL rated Fire doors, etc.).

For example, consider the distance between a card reader and the swing of a door upon a card read. Will the swing of the door make it awkward for the card holder to gain entry after scanning a card? Would a card reader located on the door frame itself or with a longer read range make the opening easier to use?

A low-level perspective is important during the design and installation phases of implementing an access control system, especially in how the access control system impacts the usability of the door.

## Steel Doors

In the commercial architectural market, 'hollow-core steel doors' and 'steel frames' are a mainstay product. Many access controlled doors fall



into this category; the products are typically constructed of 16 - 22 gauge steel sheeting and then cut, formed, and welded into assemblies. 'Hollow core' indicates a steel shell with a fiber composition or polystyrene honeycomb core.

Steel doors provide a good rigid medium to hang a variety of security hardware upon. However, over time the perpetual hanging and rehanging of different types of hardware can damage the door and result in a structurally unsecureable opening. For example, make sure that maglocks are mounted with 'thru-bolts' and not only surface mounted.

While a steel door allows for mounting various accessories, this can result in awkward interaction of mechanical devices and access control systems. If the intent of an opening is to open upon a card read, make sure that no existing mechanical device (ie - deadlatching exit device) prevents this action.



### Wood doors

'Wood veneer', or 'solid core wood' doors are also very common, especially in institutional and education buildings. The term is self-explanatory; instead of a hollow-core steel door, one composed of wood or wood veneer is used in its place. These types of doors are still commonly installed in steel frames.

Surface mounting hardware like maglocks to wood doors can sometimes be troublesome. Not only are those finishes especially sensitive to damage like tool marking and hole break-outs but the actual door itself will 'move' depending on environmental variables like heat and humidity. Because of that, special care should be taken to mount hardware so that it will always remain aligned, i.e. - a good electromagnetic bond is achieved.

## Glass Doors

Glass Doors, sometimes referred to generically by specific brand 'Herculite', are very common in architecturally significant openings like storefronts or main entries into highrise structures. These types of doors usually present cosmetic constraints to hardware specification, and due to the thin frame, or frameless, opening types great care must be taken to ensure the constraints of movement and interaction of hardware is well understood.



These types of doors are especially costly to modify in the field if improperly configured. Often times, the glass must be cut during manufacturing to accommodate for items like hardware and hinges. Making sure the build and action of these doors is understood will ensure cost controls when working with them. See [Glass Doors and Access Control Tutorial](#) for more on this often difficult combo.

Electromagnetic locks are most commonly used in glass doors rather than strikes. A variety of factors account for this: these doors see high traffic counts and strikes are more burdensome to maintain than electromagnetic locks, and it is difficult to 'hide' the strike in such a way that is aesthetically pleasing.

## Automatic Sliding Doors



Another type of commercial opening designed for high volume throughput are sliding doors, where an operator moves door leaves laterally rather than swing them in or out. In many markets, these types of doors are serviced, maintained, and installed by specialty vendors like [Stanley Security](#) who have exclusive service contracts for them, and integrating them with access often requires a joint effort with those providers.

Because of the complexity in configuring these doors, critical values like close time or sensor activation points must also often be included in access door controller configurations.

### Overhead/Rollup Doors

Finally, traditional overhead doors are commonly connected to electronic access for vehicle or loading dock applications. In many cases, the door segments roll upward into a coil a fraction of the height of the extended door.

Because the action of the door is not a swinging type, the arrangement of standard components (ie: door position switches) require alternative mounting locations like floor mounting. Not all rollup types use automatic operators to raise, and some use conventional bolt locks to secure, while other automatic types may require logic programming delays to ensure doors are unlocked before raising actions are activated.



### Reading Door/Hardware Schedules

The standard method of expressing door, frame, and lock details are done via schedules that are part of drawing sets. Usually, in a near complete or '100%' set of floorplans, a sheet showing a chart of door details and elevation views is included.

The 'schedule' is typically a spreadsheet-style breakdown of all door details, especially components or details not easily shown in a set of floorplans. An example breakdown of the door schedule looks like this:

DOOR/OPENING						FRAME			HARDWARE SET	LABEL/RATING	REMARKS
NUMBER	ROOM NAME/LOCATION	TYPE	SIZE	MATERIAL	FINISH	MATERIAL	HEAD	JAMB			
(100)	ENTRY	2	3'-0" x 7'-0" x 1 3/4"	EXISTING	P-1	H.M.	B	A	100	N/A	INSTALL "EMPLOYEES ONLY" SIGN PROVIDE KICKPLATES ON BOTH SIDES PROVIDE NEW KICKPLATE IN DIRECTION OF TRAVEL ONLY
(101)	ENTRY	2	3'-0" x 7'-0" x 1 3/4"	EXISTING	P-1	H.M.	A	A	101	N/A	INSTALL "EMPLOYEES ONLY" SIGN PROVIDE KICKPLATES ON BOTH SIDES
(102)	ENTRY	EXISTING	EXISTING TO REMAIN	EXISTING	P-1	EXISTING	EXISTING	EXISTING	102	N/A	INSTALL "EMPLOYEES ONLY" SIGN PROVIDE KICKPLATES ON BOTH SIDES

Door Location /Room Number
Door Construction Details & Dimensions
Frame Construction Details
Matching Door Lock /Hardware Sets

Note that important access control details like 'hardware set', which typically includes lock details, may be condensed itself into a note. Verification of details using a plan's door schedule is the best method, but still may require cross-checking multiple plan sheets and pages.

The sample schedule plan sheet below shows how the actual spreadsheet grid is shown on a floorplan sheet, often also with illustrations depicting elevation views of the actual doors in the building:

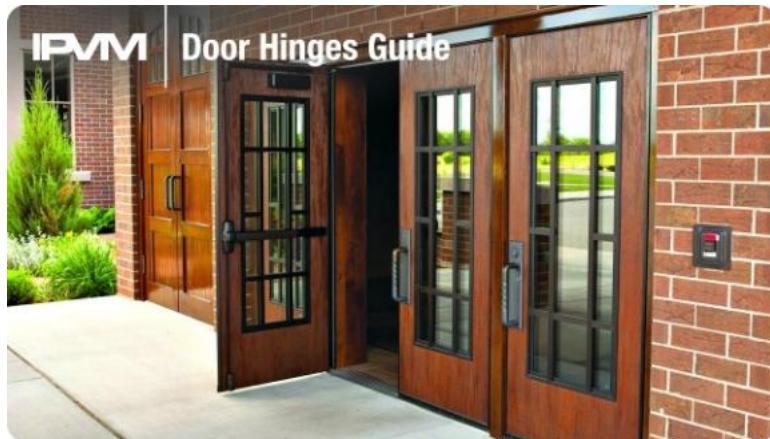
IPVM

## **Door Schedule Plan Sheets**

The illustrations are helpful for builders and tradespeople (like integrators), but the only aspect of the sheet that is standard is the non-graphic schedule spreadsheet, so familiarity reading them is a needed skill.

# Door Hinges

Some of the trickiest access control problems are caused by bad door hinges.



From doors not closing right, to locks not locking, worn or warped hinges are one of the most common root causes but typically ignored. Along with proper [Door and Frame Alignment](#), hinges often ensure that access locks properly function to keep doors locked and safely unlock when needed.

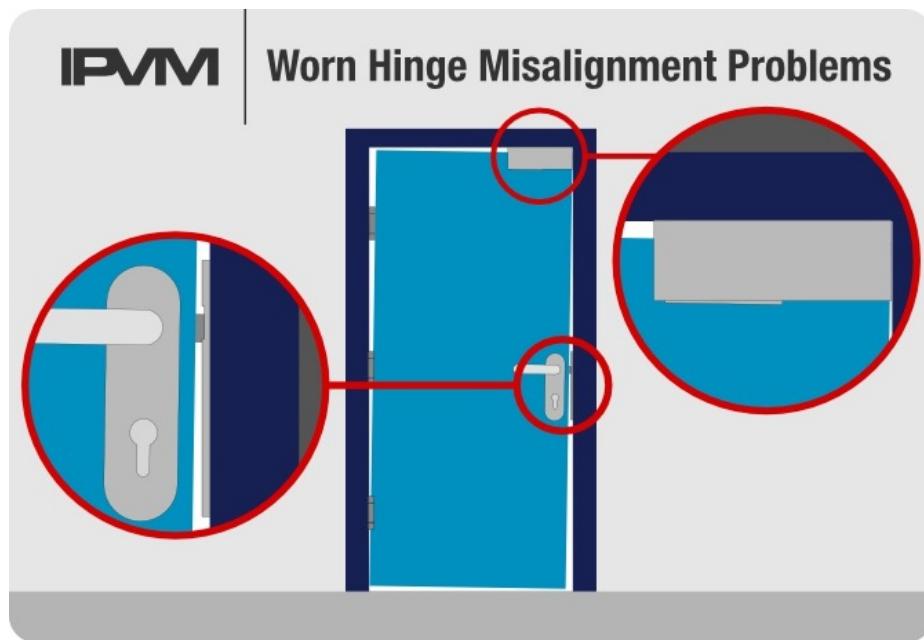
We examine:

- The 5 Access Problems Caused By Bad Hinges
- Common Commercial Hinge Types
- Butt Hinges Often Have A Big Security Weakness
- How To Mitigate Removing Hinge Pin Vulnerabilities
- Geared Hinges Are Strongest but Most Costly
- Why Power Pass-Thru Hinges Are Popular For Access

## 5 Access Problems Caused By Bad Hinges

Door hinges are devices that control how a door swings and moves and especially how closing happens. Hinges bear the weight of the door in the frame, and while routine maintenance is often applied to locks and keys, hinge maintenance is frequently ignored.

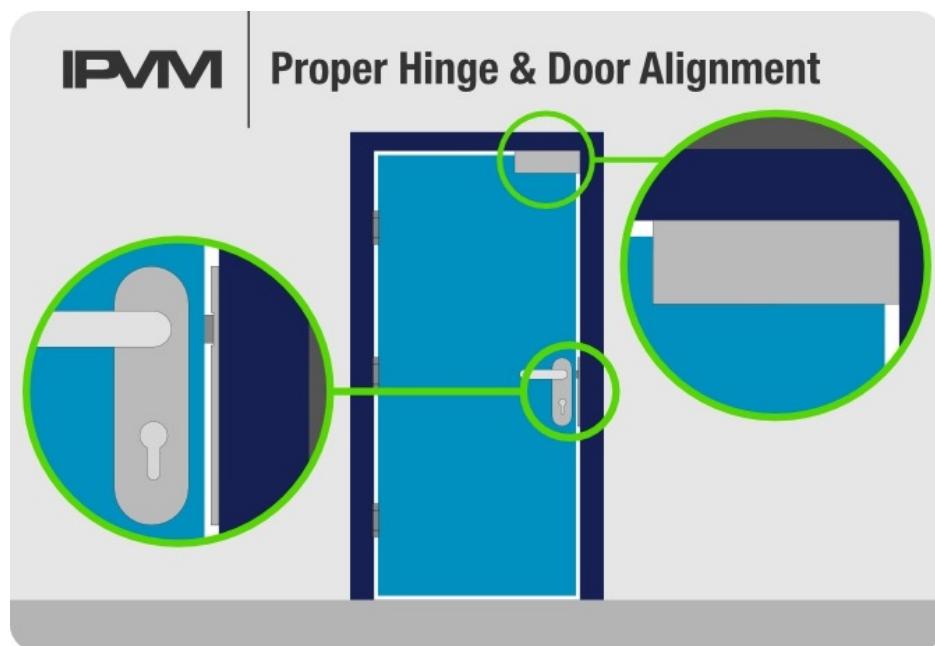
Over the span of multiple years, door hinges often wear, break down, and even bend out of shape causing a number of issues that make electronic access control tough. The image below shows five common ones:



- *Lock Latch Alignment*: When lock latches are not perpendicular to the strike, they often cannot extend fully and may even get stuck or be damaged in typical use.
- *Binding Strikes*: When a latch presses against the keeper or jaws of an electric strike, it often cannot operate freely in a condition called 'preloading', potentially even becoming a life/safety problem.
- *Weak Maglock Bonds*: Even if allowed by code, maglock strength can be significantly weakened through misalignment of the armature on the door and magnet on the frame.

- *Sticky Doors:* Typically, if one part of the door 'sticks' in the frame during opening and closing, the remedy is not 'shaving' or trimming the interfering part of the door. It is fixed by adjusting or shimming the hinge adjacent to the sticking.
- *Warped Swinging:* If some, but not all hinges are worn, then the Door Leaf itself can swing such that part of the door swings out of sync with the rest of it, potentially causing operation or timing issues with connected locks.

When hinges are undamaged and installed properly, the issues above are typically remedied, i.e.:



A sure check of good alignment is a uniform gap between the edge of the door and frame on all sides. This gap, usually between  $1/4"$  -  $3/8"$  (0.635 cm - 0.9525 cm) depends on the door material and door size/weight, but the gap should measure the same near the floor as it does near the top edge.

When this gap tapers, it often indicates the screws holding the hinges at the very least need to be adjusted, and may even signal that advanced repairs like shimming, or even hinge replacement are needed.

We examine this detail in our [Door and Frame Alignment Primer](#).

### Hinge Configurations Typically Factory Set

In most cases, commercial doors will have three to five hinges and are specifically fabricated with certain hinge performance in mind. Most doors use three hinges, but heavy or tall doors often use five sets.

The door designer often specifies which type and how many sets of hinges are used when the building is initially built. However, as operational demands of the building change over time and as each door is used at a different rate, some door hinges may wear out or become maladjusted compared to other identical sets.

For this reason, installers and those servicing access control should also be familiar with checking and adjusting hinges as part of their scope. Because hinge configurations are typically factory fixed, replacing them is picking duplicates. However, understanding the basic types and options is crucial when ordering replacements or optimizing them for access use.

### Common Hinge Types

In commercial use, hinges are designed to bear both the weight and swing action of door, often hundreds of pounds.

- *Butt Hinges*: The most common type of hinge is the most desirable combination of low cost, easy replacement, and durable use for most openings.
- *Continuous/Geared*: However, for doors with high volume and damaging use, full-length and highly durable geared hinges are used, but at a much higher relative cost than butt-hinge types.
- *Lift-Offs*: Some hinges are designed so the door can be temporarily removed to expand opening space by using 'lift-off' hinges held normally in place by gravity and door weight. Because they do 'lift-off', they are not good for securing openings and often must be replaced if used on security perimeter doors.

- *Pivots*: For glass or storefront openings, conventional hinges are typically replaced by specialty 'pivots' designed specifically for the openings and are not interchangeable in service or replacement.

### **Butt Hinges Most Common**

The most popular type of hinges used are 'butt hinges', designed to fit into slight pockets in doors and frames and with a freedom of travel of 180 degrees or more. Common commercial units are often fitted with sealed ball bearings and attached using a pattern of four or five bolts to frames and leaves:



For commercial use, a single set of butt hinges cost ~\$10 - \$20 per set, so the total to outfit a single door with multiple sets typically ranges ~\$40 - \$80 in hinges per door, although specialty butt hinges may run up to several hundred dollars per door.

In most cases, the pivot side is located inside, or on the protected side to minimize tampering risk. Depending on [Door Swing](#), hiding the pivot inside may not be possible so other variations must be used, including:



'Swinging Butt' hinges are often used where the swing of the door or location of the pivot must be opposite the shortest path, often across the thickness of the door itself. Yet, the hinge is designed to bear the weight evenly despite being cantilevered in the frame.

### Security Features

Another important feature for hinges, especially those with exposed pivots, is how easily the hinge pins can be removed. Removing the main pins allows for the hinge to be separated into halves, potentially allowing the door to be removed and for access to be gained by unauthorized people.

Certain types of hinges are especially vulnerable to this type of attack, especially decorative hinges with over-sized and decorative ends on hinge pins, like this example:



Using common hand-tools like channel locks or pliers allow vandals to take hinge pin tops off and allow for easy removal of the main hinge pin. In most cases the pin can be taken out by tapping it free or using common materials like nails or punches to knock pins free:



Many types of commercial hinges include sealed ends specifically designed to destroy the hinge before the pin can be removed, or do not use a main pivot hinge pin at all. However, normal hinges can mitigate the risk with additional 'security pins' that keep the door locked in closed position even when the hinge pins are removed:



## **Geared Hinges Best, Most Costly**

For openings that encounter heavy use where the doors are opened or closed forcefully many times per hour, crashed into by carts, or even forcefully slammed by winds, normal butt or pocket hinges may wear out in just a few months.

For these openings, 'Continuous Hinges' also called 'Piano' or 'Geared' hinges are a good solution. This type of hinge is the most durable and most resistant to damage, and typically runs the entire height of the door to which it is attached.



Because these hinges are the most materially substantial, and because they require the most labor to install, they are often the most expensive, costing ~\$500 - \$750 per door. The image below shows how they typically look when installed, covering the entire length of the hinged side:



In general, geared hinges eliminate common alignment issues by making the entire hinge side of the door part of the hinge surface, so surface or mortise mounted locks often have the most repeatable and dependable operation.

### Special Features

Hinges are not only just mechanical. Some hinges, like 'power pass thru' hinges actually route power for locksets or exit devices through the moving pivot of the door, greatly simplifying and protecting the low-voltage conductors need to power access locks.

These hinges often look 'normal' with the exception of wires leading from the mounting plates:



While 'pass-thru' hinges are often valued for making power delivery easier, they often malfunction and wires can easily break over time/ cycles of use, and may require replacement at a more frequent pace than non-powered types.

# Specifying Door Locks

Mechanical door locks regularly remain even after electronic access control is added. Indeed, most are designed to work with what is already hung on the door. However, what happens when a lock needs to be replaced or changed? Understanding the basics of selecting and installing door locks is valuable for every designer, installer, or end user to know. In this note, we take a look at the basic types of locking hardware, which types of openings use them, and provide a general overview of how to install them.

## Major Types

The range of lock hardware is broad, with each type having its own 'best use' and relative strengths. The major types used in commercial buildings are shown below:



In the sections below, we discuss where each type is used and how to make the best choice depending on the application.

## Door Preps Largely Decide Lock Choice

The most important aspect driving door lock selection is how the 'door is prepped', or how it has been fabricated to work with locks. Different forms of locks require different configurations of holes and pockets cut into the door, and in most cases these preps are done at the manufacturer well before they are hung.

Therefore, in many cases, lock selection is decided by the door type, and the task is condensed to finding which product can be installed without modifying or replacing the door. In the sections below, we address the major types of 'door preps' and which models of hardware they accept.

### Cylindrical

This type of lock is also called a "Bored" lock, which essentially is designed to slip inside a 2 1/8" hole drilled thru the door. The locks designed to use this prep are round in shape, and typically use the hole to support the lock in the door. While the majority of doors include this prep, it is not the most common seen in Electronic Access Control, because most of the time these locks are used for interior, or low-security doors.

While these types of locks are well suited for light-duty use, they contain only one latch - the piece that slides into the frame. High security doors often include several points of latching and even when a cylindrical lock is built to withstand many cycles, it still need other separate components (like a deadbolt) for high security applications.



**Cylindrical Door Prep / Leverset**

- *Pros:* Inexpensive (\$50 - \$300), easy to install
- *Cons:* Single latch not as secure as other types, not as durable as mortise locks
- *Where Used:* Interior Doors, Offices, Passageways, Low-Medium Volume Doors

## Mortise

One of the oldest types of locks is also the most secure. Compared to a cylindrical lock, a mortise lock is big, heavy, and full of complex parts. However those properties make it very durable, strong, and able to withstand constant use. Mortise locks require a pocket cut into the edge of the door, which requires more craft skill than a single bored hole. However, because that pocket is larger than a cylindrical lock, multiple latches are typical features of mortise hardware.

Not only do multiple bolts slide into the frame, but mortise locks support full-size 'high security' mortise lock cylinders featuring 'bump/pick resistance', special security pinning, and other tampering protections.

Mortise locks are commonly used in doors requiring high security and high volumes, but are generally too expensive to use on interior doors or light-duty office/ passageway openings. Doors using mortise hardware must be specified to handle both the size and weight of a mortise lock:



- *Pros:* Very durable, support multiple security latches
- *Cons:* Expensive (\$400 - \$2000), field cutting a door to support a mortise lock is difficult
- *Where Used:* Exterior Doors, High Volume Doors, High Security Doors

## Surface

Also called 'Rim style, or Edge-prepped Locks', these locks typically require minimal door prep, and some types do not even occupy the core of a door at all. The most common type of hardware in this category are [exit devices](#), a mainstay of high-volume, emergency egress openings. In the picture below, notice the latch of the lock is attached to the 'surface' of the door, hence the name:



Surface door hardware is typically secured with surface strikes (not mortise strikes) or maglocks where permitted. Exit devices are costly but are very durable and typically withstand high amounts of abuse and tampering.

- *Pros:* [Meets Life/Safety Emergency Egress Codes](#), Most doors, regardless of factory prep, support Surface Hardware installation
- *Cons:* Expensive (\$1000 - \$3000), and potentially disruptive to aesthetics. Difficult to hang on glass doors.
- *Where Used:* Egress Doors, High Security Doors

## Deadbolts

This type of lock is seldom used alone without additional separate handles, and NEVER on emergency egress doors [link no longer available] because the bolt typically requires rotation of a key or thumbturn to retract. Like cylindrical locks, deadbolts are easy to install, requiring only a hole to be drilled through the door. However, because of their limited convenience, deadbolts are primarily used to enhance the security of other locks hung on the door.

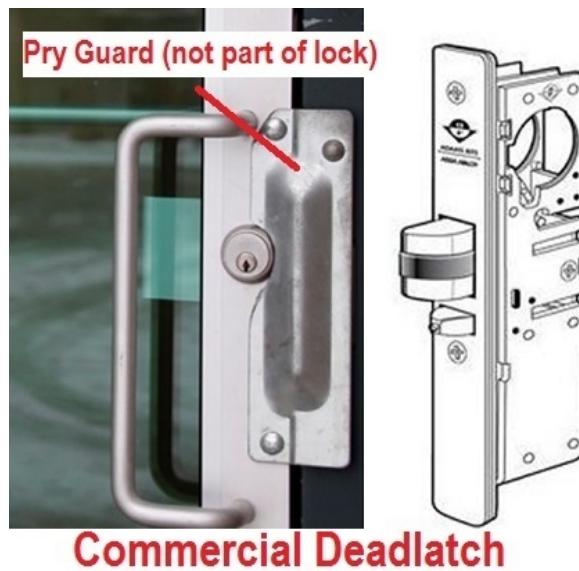
For example, when used with a cylindrical lock, a deadbolt means another independent lock must be defeated to gain illicit access. Deadbolts are typically used to increase security during 'dark hours' - used when a facility is locked up for the night or when it is unoccupied. The image below shows a typical example of how deadbolts are used, in conjunction with a leverset on a perimeter door:



- *Pros:* Inexpensive (\$50 - \$200), easy to install
- *Cons:* Cannot be installed on egress doors, Separate lock must be pinned to match other locks in use
- *Where Used:* Generally used to increase security by provide another latching point.

## Deadlatch

This type of hardware is a hybrid between a deadbolt and a mortise lockset. Deadlatches are commonly used on glass storefront doors with thin frames. Most properties using latchbolt equipped doors are unlocked during occupied hours [link no longer available], and free egress and entrance is permitted. Therefore, a latchbolt is only used to keep a door locked when occupants are gone. Like a deadbolt, most models lack handles to retract the latch, although some types feature '[exit device'-like paddles](#) when required by code. Unlike a deadbolt, a door frame cannot simply have a bored hole for install, and the frame must be prepped similarly to a mortise style lock. Most latchbolts are very strong, and may include multiple latches or [even hook bolts](#) that anchor firmly into the adjoining frame.



- *Pros:* Stronger than traditional deadbolts, the ideal architectural/security compromise for glass doors
- *Cons:* Handles must be installed separately, retraction functions from key only. Doors difficult to field prep to fit latchbolts.
- *Where Used:* Thin Frame (Glass) Storefronts

## Lock Selection

Doors clearly drive the types of locks that can be used to secure them. When it comes to selecting the specific type of lock to install, these factors:

- *How is the Door Prepped?* The section above clearly defines how door prep influences lock hardware selection. Taking note of the prep will narrow selection criteria to a few basic types.
- *How thick is the door?* Doors have varying thicknesses. In the Americas, doors usually are 1.75" or 1.375". However, European models range between 30mm and 55mm thick. This measurement is critical in determining the latch position in the door, and can limit the overall thickness of the lock.
- *Is this an Egress door?* If the door falls in an egress or emergency egress path, certain lock types (like deadbolts) should not be used. Hardware like exit devices maybe be required, excluding selection of other types.
- *How do codes affect lock selection?* Many municipalities outlaw maglocks, meaning that 'electrified hardware or strikes must be used. Local code interpretations often exclude types of locks, or otherwise conditionally approve their use depending on building classification.
- *How frequently will this door be used?* How often the door and lock is cycled [influences hardware grading](#). For heavy duty commercial use, ANSI/BHMI Grade 1 hardware is ideal, while an infrequently used closet or storage door is better suited to use economy-grade Grade 3 hardware.

Choosing the right lock is typically driven by the 'context' attributes of the opening, rather than selecting the lock first and sizing the opening to fit.

# Door Swing

The direction a door swings might seem minor, but it can greatly impact door hardware selection.

There are four basic ways a door can swing, and knowing how to properly determine it is critical when designing access control systems and ordering door hardware.



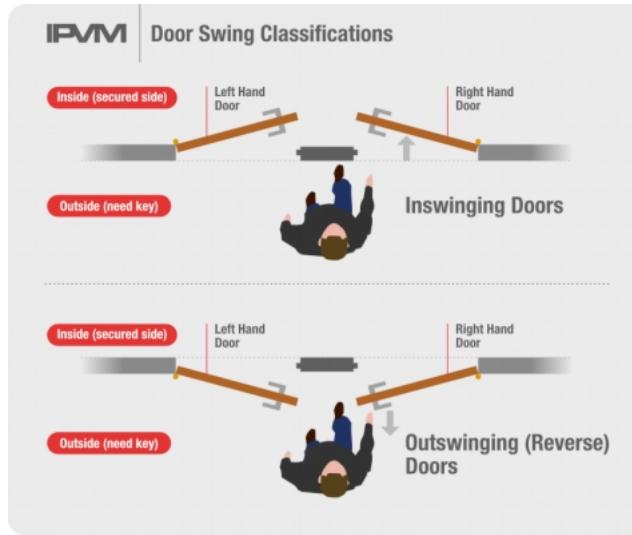
We lay out how to describe doors based on this subtle but divisive characteristic.

## Door Swing Defined

Openings are configured to have doors swing in four separate ways:

- *Right Hand*
- *Left Hand*
- *Right Hand Reverse*
- *Left Hand Reverse*

The differences in these types are best described with diagrams. The images below show all four types:



## How To Find Door Swing

You can describe any door using this standard by following these steps:

[Click here to view the Door Swing video on IPVM](#)

- Stand Outside the door, on the locked or public side.
- Check which side the door hinges are located. This direction, left or right, describes the direction.
- Next check to see if the door swings in (away from you) or out (towards you). If the door swings out, it is a 'reverse' type.

Describing doors in this manner is standard in architecture and is the same nomenclature used by engineers, specifiers, and access control.

We show this in action in this short video:

## Why Swing Matters

Properly defining door swing is critical when ordering and installing door hardware, like cylinder locks, and access control components like maglocks. Incorrect door handing result in keyed

locks on the wrong side of the door, lever handles that are upside down/ point in the wrong direction, or maglocks being installed on the 'wrong side' of the door.

## Maglock Specification

Door Swing plays a key role in mounting maglocks. Take the example images below:

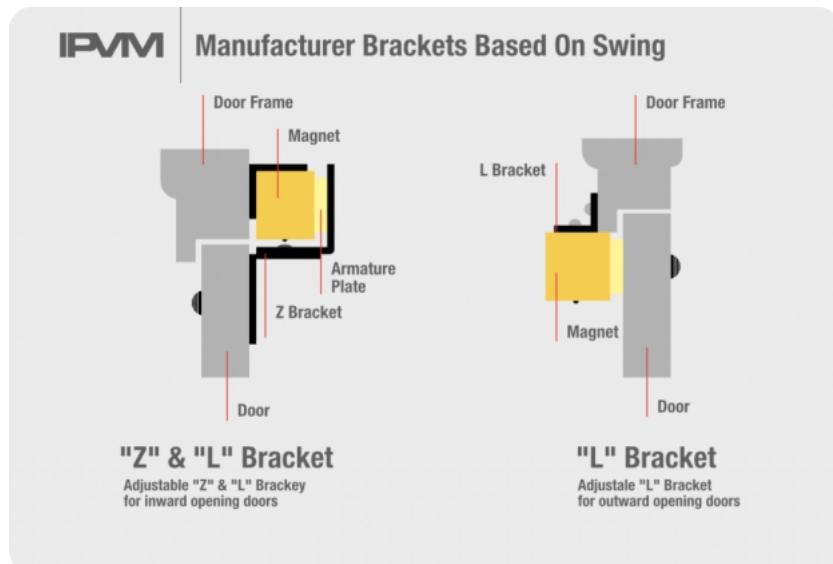


The left image shows a typical egress door that swings out. These doors typically have exit devices and swing out towards the unsecured side so that panicked people trying to evacuate a building do not need to swing the door towards them to open it. If the door did not swing out, people could potentially be crushed against it trying to escape.

The image below shows an inswinging door. The maglock magnet cannot be mounted on the frame, because it would need to be mounted in an exposed manner on the outside of the door:

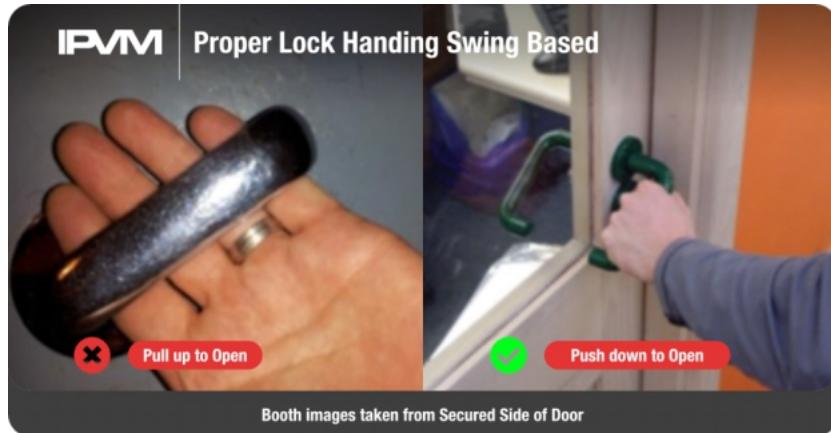


To prevent this issue, maglocks must be ordered with additional brackets, typically called "L" or "Z" brackets. The only method of determining if these brackets are needed is to note the swing direction, and inadvertently omitting them from a job estimate can cost hundreds or thousands in additional hardware and labor.



## Door Lock Handing

The other major specification affected by door swinging direction is the 'handing' of a door lock. This affects which direction the lever handle must travel (or which direction the knob rotates) to unlock the door.



In order to meet code, the door must open when the handle is pushed down, and not all hardware retracts the latch if the handle is worked in either direction. The video below explains the difference:

[Click here to view the Lock Handling video on IPVM](#)

Most door locks, including standalone electronic access control locks, are 'field handable', which means they can be configured at the jobsite to work in any type of opening. However, this process takes time, usually 15 to 30 minutes for each lockset, and over the course of many doors this process can add hours of unexpected labor to a job. Manufacturers will sell door locks pre handed for the same price, and ordering according to the preset handing is valuable when door swing is noted during design.

[Note: this tutorial was originally published in 2013 but was substantially revised in 2018.]

## Maglock Selection

One of the most misunderstood yet valuable pieces of electrified hardware is the maglock. Few locks are stronger, but myths and confusion surround their proper use.



Many access control designers avoid using them altogether, but should they? We examine maglocks, their proper application, and how to avoid problems when using them, including:

- Fail Safe vs Fail Secure Concerns
- The Core Components of a Maglock
- Legality of Maglocks, Per Code
- Shear vs Conventional Pull Action options
- Bond Ratings
- Power Considerations
- Matching Maglock to Door Operation
- Maglocks and Glass Doors
- Why Using MOVs/Diodes Is Important
- RTE / Fire Alarm Considerations

## Designed to Fail Safe

Despite misconceptions about their safety, all maglocks 'fail safe', or become unlocked when power to them fails. Because a maglock is an electromagnet, if energy is not present, it simply does not operate. By design, maglocks lose all holding force when power to them drops.

Other types electrified locks may be configured to 'fail secure', or stay locked when power fails. However, this can complicate egress in an emergency. Maglocks do not have this issue.

In contrast to electronic cylinders or electric strikes that have moving mechanical components that can break or bind, a maglock has no moving pieces and does not wear over time. The 'solid state' construction means that a maglock either operates according to design, or it does not operate at all.

## Two Basic Maglock Components

Despite their 'high-tech' latching method, a maglock is a simple device composed of just two pieces:



- **Armature:** This is a flat section of steel that matches the magnet 'box' installed on the frame. The armature must be securely fastened to the door in order to achieve a strong bond and keep the door shut.

- *Magnet*: The larger of the two components contains an electromagnet core. Unlike the armature, this piece never physically moves in relation to door swing, and is the only component that receives power during operation.

## Other Maglock Options

While not essential to keep doors secured, maglocks are often equipped with or require additional components that aid their function in access control deployments. Among these other elements are:

- *Bond Sensor*: A simple contact closure than confirms the maglock is energized and matched with the armature, signalling a valid 'bond'. This indicates the door is both closed and locked/secure.
- *Integrated RTE PIR or REX*: (*Request to EXit Motion Sensor*): Some maglocks include a motion sensor or switch that drops power to the lock. This feature is required by life/safety codes so that in an emergency egress situation the lock drops power and permits exit. The image below is an example of this type:



## Which Maglock Should I Choose?

Selecting the proper type of maglock for an application is not difficult, if a few basic parameters are addressed during specification.

The basic questions that must be answered, and the order they must be asked are listed below:

- Legality/ AHJ requirements
- Action Type (Shear vs. "Conventional"/Pull)
- Bond Ratings
- Voltage Type
- Operation Type
- Required RTE Hardware/Fire Alarm Tie-In

### **Legality/ AHJ Requirements**

The first, and most critical aspect that must be addressed is whether or not use of maglocks are permitted by the local code authorities, or what special restrictions apply to their use.

National model codes, like IBC and NFPA 101 do not prohibit using maglocks, but they still are not legal in many areas.

Codes require integration between the fire alarm systems and maglock controlled doors to become unlocked when alarms are activated. Concern and uncertainty about this integration leads many local AHJ and local codes to forbid maglock use anywhere, while others may limit use in certain building occupancies.

Maglock prohibition is usually passed on a municipal level, and can vary from one town to the next. In general, a call to the local Fire Marshal or City Codes department will yield proper guidelines. In the examples below, note that accepted use may vary depending on door locations, door types, and maglock type:

- [New York State](#) (Education Dept.)
- [City of Chicago](#)
- [Harris County](#) (Houston), Texas

In many cases, more 'elegant' and aesthetically pleasing access options for securing doors exist, and many installers and end users alike seek alternatives to maglocks even when code allows.

## Shear Action vs. "Conventional"/Pull Action

Maglocks are available in two functional types; either Conventional/Pull style or Shear style actions. The difference between these types is noted in the drawing below:



The action determines the intended mounting location of the maglock. The movement direction the lock is designed to 'hold' distinguishes the type. Because of the differences in coil windings, a 'conventional' maglock is not suited for use in a 'shear' application, and vice versa.

While the operating principle is the same, the installation locations and door preparations are different according to maglock types. In the sections below, we address the two types and how they differ.

### Conventional / Pull Locks

The most common type of maglock installed today is the "Conventional/Pull" type.

In contrast to the shear action, this type is installed with the magnet exposed, meaning the magnet must be installed on the 'secure' (or unexposed) side of the door.



The [direction of door swing](#) complicates mounting position, since some doors will swing in - resulting in a modification to the installation position and armature bracket, because the swing of the door would interfere with the lock if hung in the 'outswinging' position.

For inswinging doors, the lock is moved up and mounted flush with the side of the top frame. In addition, the armature is moved outward and upward with a 'z-bracket', which may be an additional cost. Note in the picture below how the door swing affects installation location:



For all conventional style maglocks, the armature plate is installed flush onto the door itself, typically attached with through-bolts to the door. While not an issue for hollow metal or wood doors, this can present a problem for frameless glass or thin bezel doors.

### **Shear Locks**

This style of maglocks is ideally used where maglocks must be low-profile, as they can be completely recessed (hidden) into frames.

Because these units are installed flush with exposed surfaces, they are tamper-resistant. However, shear style locks are less common than the 'conventional' type because both frames and doors must be previously fabricated with lock clearances in mind.



Since most electronic access control systems are retrofitted to existing doors and frames (without the proper cut-outs), shear locks are not frequently used. Also, the position of the door armature must also be aligned under the lock, which requires regular adjustment of the door.

However, because of their low-profile and strong bond in the intended direction of travel, special applications like gates or rolling grilles often employ shear locks.

Cost for shear locks is roughly equal compared to other maglock types, however due to the additional fabrication required to doors and frames to fit them, the deployment cost is higher.

### **Maglock Bond Ratings**

Despite their disadvantages, maglocks are among the 'strongest' locks available.

Maglock 'strength,' or holding force, is measured in hundreds of pounds, frequently more than 1,500 pounds per lock. This rating describes the amount of pulling force required to match the magnetic bond of the lock, and greater amounts of force are needed to overcome it.

Typically, the lowest bond rating available is 600 pounds, while the strongest models are rated to 2,700 pounds or more. In general, the stronger the holding force the higher the cost anywhere from a few hundred dollars to more than ~\$1,800 for the strongest units.

However, considering the structural elements of the door, (eg: leaf, frames, pull hardware) will fail before the maglock itself, it is exceedingly difficult and uncommon for the bond of a maglock to be defeated.

### **Minimum Bond Needed For Exterior Doors**

In general, exterior doors should not be secured with less than 1,500 pound rated maglocks.

Less expensive and weaker locks have a variety of uses (eg: securing cabinet doors, sliding gates, or closets), but they should not be used where a brute force attack using tow chains or mechanical come-alongs is possible.

## **Power Considerations**

Most maglocks are field selectable to either 12 or 24VDC, but other voltages and AC rectified versions are available. Power for these locks is often recommended to be supplied by an independent, individually fused power supply.

Because the effectiveness of these locks is entirely dependent on the strength and dependability of the power source, maglocks do not typically share power sources with surveillance equipment.

Unlike locks that intermittently draw power when activated, a maglock continually draws power during operation. The heavier duty-cycle of the maglock calls for a supply source that is more robustly built and able to handle the constant supply of current to the lock.

## **Double-Door Units**

Maglocks can be installed on 'dual-leaf' or 'double-doors'. Typically codes require adjacent door leafs to release simultaneously. While this can sometimes be achieved with two single-door maglocks, many electronic access door controllers are only able to be connected to a single locking device.

In this case, a double-door unit must be used so a single release command will allow adjacent doors to open at the same time. The image below shows a double or 'dual-ganged' maglock:



## Difficult Mounting Locations

Installing maglocks can be difficult in typical doors given the clearance needed to install the armature, brackets, and bond area of the magnet to match.

The location on doors where maglocks are mounted, typically the top where [Door Closers](#) and [Door Operators](#) are located can make for difficult installation.

In the picture below, note the armature size and the corresponding size of the small magnet used due to the large footprint of the operators:



In this case, using maglocks of such small size may prove not strong enough to truly secure the opening, and [other locks are better used](#).

Even the profile of the frame itself can present mounting problems, and often spacer plates or reinforcing brackets are needed to mount maglocks securely for access use.

## Hold-Open Function

Variants of maglocks are also used to hold doors open. Especially in applications like hospital corridors or busy hallways, fire doors are critical openings that must be closed to be effective during a fire, but otherwise are seldom closed during regular use.

Because maglocks can easily be integrated into fire alarm systems, they are often used to lock doors in the 'open' position, and in a fire-alarm situation, the maglocks release and associated door closer then shuts the doors. The image below shows magnetic 'hold opens' used in this application:

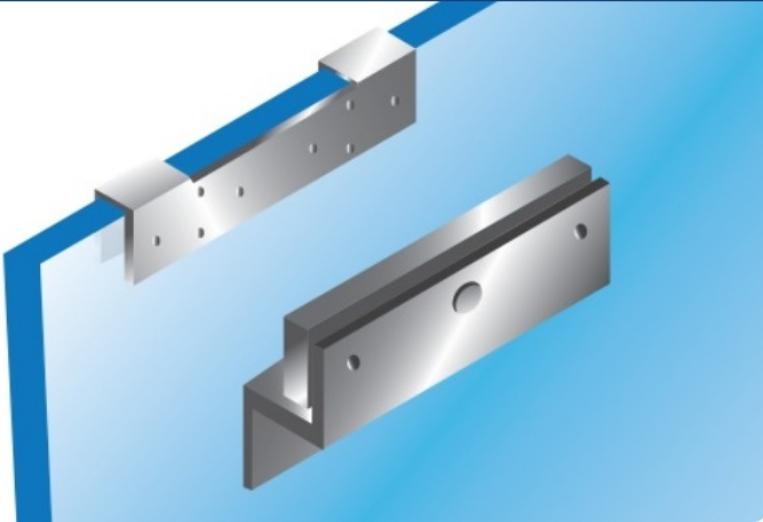


### Glass Doors And Maglocks

One of the more difficult locations to install maglocks are glass doors with thin or no frames.

Because tempered glass cannot be drilled in the field without tremendous risk of shattering, many maglock 'glass kits' include brackets that must be glued or clamped into place, like the ones shown in the image below:

## Glass Door Armature Brackets Needed **IPVM**



See our [Glass Doors and Access Control Tutorial](#) for more on this tough application, including alternatives to maglocks.

### Metal Oxide Varistors/ Diodes Stop Damage

Because a maglock causes a magnetic field to collapse every time it is de-energized, it can backfeed a small but damaging surge into the power supply. A diode or MOV dissipates this field and prevents this type of damage from happening.

If not factory equipped, [the maglock may require these components to be field installed](#), typically across the power leads of the lock.

### Required RTE Hardware/ Fire Alarm Tie-In

'RTE', or 'Request to Exit' Hardware, are typically PIR motion sensors and/or 'Exit' pushbuttons, that must be installed so a maglock unlocks when people want to egress through the door. The image below illustrates common RTE devices:



For more, see our [Access Control Request to Exit \(RTE\) Tutorial](#).

### Battery Backup For Maglocks

Codes do not forbid using batteries or UPS to provide power when main building power fails.

Indeed, a weakness of 'fail safe' locks like maglocks is that doors they secure fall insecure when power drops. Using battery backups can mitigate this weakness.

However, any batteries and safety interlocks with fire alarms should be designed and installed properly. We cover the finer details of compliant methods in: [Backup Power For Maglocks Guide](#).

[NOTE: This guide was initially published in 2012, but updated and expanded in 2019.]

# Selecting the Right Electric Strike

Despite being one of the most common components of access control, specifying the right electric strike can be deceptively complex. Understanding the particulars of each device can be overwhelming. We describe which characteristics of strikes are most important and how to select the right one.

## Function Explained



Strikes are basically moveable portions of the door frame, consisting of 3 main components, shown to the left:

- The Strike Box contains the internal components to the strike that sits inside the frame. Electric strikes are typically [driven by one or more solenoids](#), either directly or via a simple geared carriage inside the box.
- The Strike Plate affixes the device mechanism to the frame and is responsible for the proper alignment the device in relation to the door locking hardware.
- The Keeper is the component of the strike that moves. When 'locked', the keeper is rigid and forms a positive stop - interfering with the latch to prevent opening of the door. When 'unlocked', the keeper swings out of the way of the latch and allows the door to open.

Unlike other types of hardware, strikes do not replace or improve the existing hardware mounted on a door. In fact, a strike totally relies on mechanical door locks for securing the door. The strike simply allows for the locking hardware to remain locked and still gain entry through the opening.

*Fail Safe/Fail Secure:* Unlike maglocks that 'fail safe' on power loss, strikes can be configured to 'fail secure' - meaning the keeper remains rigid regardless if they are powered or not. In order to preserve the life/safety compliance of the opening, the door hardware must accommodate free egress in an emergency. Whether through panic bars/exit devices, lever sets, or even latch sets, egress doors cannot be locked to prevent escape, and hardware must take no more than one, intuitive action to open the door.

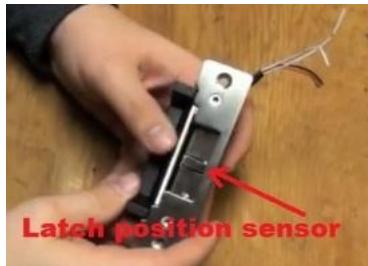
*AC or DC powered:* Most modern strikes either allow selecting between AC and DC or available in AC or DC versions. All strikes are low-voltage, with either 12 or 24 volts standard. Final polarity and voltage selection depend on several design criteria:

- *Noisy vs. Quiet:* Due to differences in the way solenoids handle power types, AC electric strikes make a characteristic 'buzzing' noise when operating, [while a DC model is quieter \(or even 'silent'\)](#). In the past, solenoid reliability was tied to polarity types, but modern strikes can be purchased to [exceed 'Grade 1' reliability](#), leaving polarity choices subject to matching existing power supplies or tolerated noise.
- *Battery Backup vs. Low Current Draw:* Since 12 VDC 'backup' batteries are common to many electronic systems, they are an inexpensive option for backup power compared to 24 volt cells. However, the current draw of 24 volt strikes is typically lower than 12 volt versions, so if multiple devices are to be powered from a single source or if overall energy consumption is a concern, 24 VDC devices are a popular choice.

*Integrated Readers:* A newer trend in strike design is [integrating a proximity-style reader into the device](#) and running both power and communication bus down a single cable. This integration allows a more streamlined installation and offers a less intrusive install by combining the reader and strike into a single unit. Variants exist that include 'read-in' and 'read-out' capability, with the unsecured side reader being connected through the frame or wall assembly via bluetooth.

*Door/Latch Monitoring:* A common option for many strikes is a latch monitor, or a simple contact switch that detects when a latch bolt is being contained inside the strike. This sensor

also functions as a defacto 'door position' contact, since the door must be shut for the latch to be present. While not all strikes feature this switch, it usually does not add significant cost to the device but greatly enhances the reporting function of the device.



## Strike Types

Selecting the right type of strike includes considering the 'form factor' of the device. Strike are available in two common types:



[Mortise](#): The most common type of strike is the mortise variety, [which typically requires a cutout in the frame](#) for install. Mortise Strikes are used when the door locking hardware is a mortise or [cylindrical lock](#) - or any other lock whose latch is retracted into the door leaf during operation. Since the bolt protrudes into the frame, a mortise strike's keeper replaces a portion of the reveal. As we will cover in the installation section, installing a mortise strike requires the strike to be installed deep into the frame, often requiring frame material to be precisely cut away for a clean fit.

[Surface](#): These types of strikes are used when the companion locking hardware is a 'rim style' device, meaning it is mounted to the inside surface of the door [link no longer available] rather than inside the door. Common 'rim' devices are 'exit devices [link no longer available]' or [surface deadbolts](#). Even though a portion of the device protrudes on the '[door rabbet](#)', the strike box may still require an additional cutout in the frame for proper mounting.

## Strikes Vs. Other Hardware

The relative value of strikes compared against other electrified hardware types

### Pros

- *Inexpensive*: Strikes are among the least costly electrified devices, with Grade 1 quality devices selling between \$100 - \$300. Compared to locks like maglocks that range between \$400 - \$ 1000 per unit. Even when considering the installation labor, the cost of a strike is between \$175 and \$375 per door.
- *Reuses Existing Hardware*: Another benefit of strikes are they are specified to work with door hardware already in use. Not only does this reduce the 'hard cost' of buying more locks, it saves on the 'soft costs' attributed to re-keying, installation labor, and redistribution of mechanical keys.
- *Energy Efficient*: Unlike maglocks that require a steady impulse of electricity to operate, a strike uses only intermittent impulses to operate. While the operational amperage is relatively small for either device, when multiplied over tens or even hundreds of doors, using strikes can cut hundreds of amps from a facility's electricity consumption.

### Cons

- *Wear*: Unlike maglocks, strikes cannot be installed once and operate for years without attention. Since electric strikes have moving parts, they can wear or break over time. Components like load springs and solenoids require periodic maintenance attention.
- *Adjustment is Vital*: Since the strike is totally dependent on the door's locking hardware for security, the relationship between strike and latch is vital and the tolerances for movement are limited. Even during the course of normal operation, door hinges sag, door frames shift, and door latches fall out of throw range of the strike. Anywhere strikes are used, a companion door maintenance problem is vital to guarantee security.

- *Extra Hardware:* In some cases, additional hardware is required to protect the strike. Take the example below, where an exposed exterior strike is vulnerable to outside tampering unless additional 'latch protectors' are installed on the door:



### **Installer Skill Required**

Properly mounting a strike takes considerable skill in precision measurement and often requires cutting metal. While the overall installation process is typically straightforward, the installer's craftsmanship and trade skills determine more than cosmetic quality - the operation of the device is affected as well.

For example, while frame cuts are simplified by the use of mounting templates included with the device, the position of the template is subject to accurate measurements and assumptions that the frames, doors, and existing hardware are square and properly mounted.



Successfully mounting a strike free of problems like "preloading [link no longer available]" (often caused by misalignment and warping of the door) requires the installer to apply a skillful eye to the door condition before beginning work, and be prepared to correct structural problems by [shimming hinges](#) or even replace a warped door leaf. Will will examine the problems, and their corrective actions in an upcoming report on "Maintaining Electrified Hardware".

# Electric Strike Installation

Follow this guide and you will install a strike correctly everytime. As we detail in this post, installing electric strikes successfully is mostly good preparation, but when done right provides years of trouble-free use. We use our [test door](#) to walk through the practical installation steps needed to get it right. Even if you never will install a strike in your life, do you know if your doors are right enough? In this note, we walk through the steps needed to get it right, everytime.

## The Steps

The process of installing strikes correctly is not complicated, but care should be taken to perform each step:

- Door/Frame Alignment
- Strike Box/Jamb Prep
- Strike Prep
- Power Connections
- Final Checks

If all the steps are followed, installing strikes can take minutes and involve minimal troubleshooting. We cover the steps in detail below:

## Door/Frame Alignment

Making sure the door and frame is aligned is a critical pre-requisite. See our [door / frame alignment tutorial](#) for background.

## **Disclaimer**

From this point forward, the tutorial focuses on frame prep and strike installation on a non-fire rated opening. While the fundamentals of operation are the same, maintaining an opening's fire rating limits strike selection and frame modification to a degree not covered here.

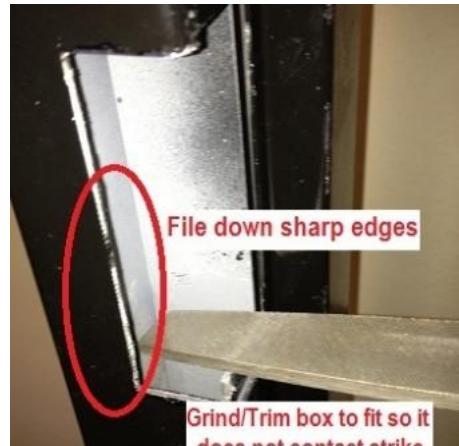
## **Strike Box Preparation**

The next step is to cut the frame so the strike fits. Even 'zero cutting' surface mount strikes used with surface hardware may require frame modification, and it's a sure step when using mortise mount strikes. We break down these steps into two parts depending on the frame:

- Factory Notched Frames
- Field Notched Frames

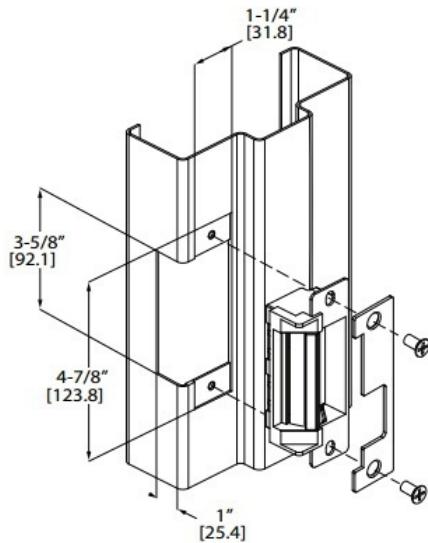
*Factory Notched Frames:* The scenario requiring the least amount of prep work is a door frame factory notched to work with a certain strike, as was the case with our door. However, even a factory notched requires filing down sharp edges and bending or adjusting mounting tabs so they do not interfere with the strike.

In our door, the strike pocket was slightly undersized so we had to use a file to enlarge the opening. When performing this step, test fitting the strike to the frame is helpful, with attention paid to potential spots where the frame touches the strike. Any pressure or tight fit can warp the strike or cause it to bind, and the strike should fit easily into the pocket.



**Preparing the Strike Box (steel)**

*Field Notched Frames:* However, many frames are not factory built to work with strikes, and more drastic modifications are required. In many cases, the existing strike box (called a [dust box](#)) needs to be cut out to make room for the new strike. The strike's installation manual generally includes specific instructions to take when modifying the frame, and the needed cuts can be made with a high-speed rotary tool (like [Dremel](#)) for steel frames or with chisels for wood. The image below is a standard example of the prep dimensions:



**Example Strike Box Prep Dimensions**

A good instructional video on how to cut out a mortise strike into a wood frame can be found below:

[Click here to watch the Mortise Strive video on IPVM](#)

### Strike Prep

After the frame has been readied, fine tuning the strike for install is next. That process follows these points:

- Fail Safe Configuration
- Trim Plate Installation (optional)
- Power Cabling

We cover these steps in the video below:

[Click here to watch the Mortise Strive video on IPVM](#)

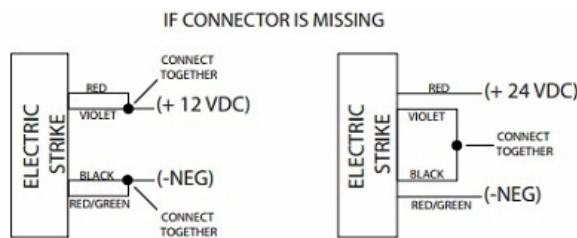
*Fail Safe Adjustment:* Many electric strikes are 'field adjustable' for either power failure condition. (For background, see our [Fail Safe vs. Fail Secure Primer](#)) Changing from one state to the other usually entails changing position of springs, solenoids, or even small levers. In the case of our strike, you must change the position of two small screws hidden under a label:



Most strike installations will use a 'fail secure' position regardless of where they are installed, and this is the default condition most are shipped with. We confirmed our strike was configured correctly, and left it as shipped.

*'Trim Plate' Installation:* For sloppy cutouts that may be unsightly or slightly oversized, most mortise strikes ship with an optional trim piece that hides the cutout. This trim, called an '[enhancer](#)' or '[skirt](#)' provides no security or operational benefit, just serves to cosmetically improve sloppy preparation work.

*Power Cabling:* Many strikes ship as 'Dual Voltage' compatible, meaning they operate given either 12 VDC or 24 VDC supplies. Some models include a dual voltage transformer in the housing with a single pigtail , while others are sold with two different pigtails trailing from the case. After confirming which supply voltage is available, the strike can be configured for use, typically involving twisting or jumping certain wire pairs together. The image below is the example wiring diagram for our strike:



## Final Installation

At this point most of the work is complete and the payoff is close. There are just a few more check to make as the strike is finally installed into the frame:

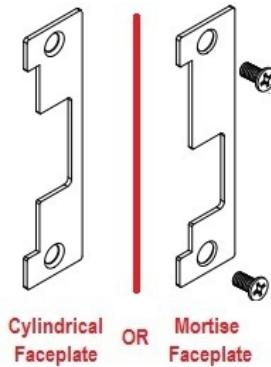
- Faceplate Selection
- Power Connections
- Installation/Shimming
- Final Function Checks

These final steps are covered in the video below:

[Click here to watch the Final Installation video on IPVM](#)

*Faceplate Selection:* Strikes generally ship with two or more faceplates, and selecting the correct one is critical during use. The 'keeper' area of the strike is bigger than the door lock's latches, and the faceplate narrows down the opening to match the specific type of door lock. This increases the 'tamper resistance' of the installation by eliminating potential gaps to insert prying tools behind the keeper.

Other door lock features, like the [deadlatch](#), need a positive surface to rest on when the door is closed, and the faceplate provides this surface. Our strike was furnished with two options, and because it will be installed with a mortise lockset, we will use the 'mortise faceplate':



*Power Connections:* Power cabling for strikes should be 'run-to' rather than 'run-from' the strike. This means that the power cablings are most easily routed from the source (typically a controller), through the frame, down into the strike box. Especially when mortar shields are prepped into the frame, the actual opening to run cable out of the box is likely difficult to find. When using a fishtape or glowrods, they can be driven up and out of the frame, taped to the end of the cables, and the power leads are drawn down into the strike area.

Once the leads are in the box, they can be connected to the strike's pigtails. The image below shows our strike, which included a factory snap-style connector for both ends of the power splice:



**Making the Power Connections**

*Installation/Shimming:* After power connections are made, the strike body should be inserted into the strike box, being careful not to pinch or crimp the cabling. If the prep beforehand has been done properly, this should be one of the easiest steps in the process:

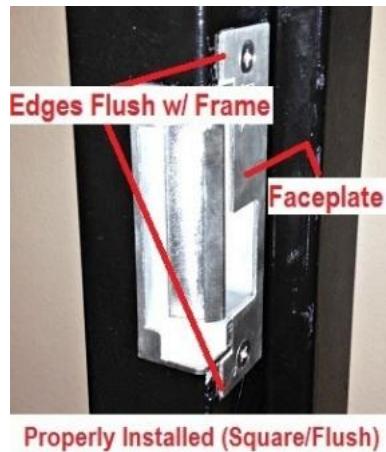


**Insert Strike into Frame**

The strike itself is not ready for use without sandwiching the faceplate down on top of the strike. At this point, with the faceplate seated onto the strike, it should be secured into the frame with the included screws or bolts. The strike itself should be square in the pocket, with no parts of the frame touching the strike except for the mounting tabs.

If the strike appears to be too far forward or too far back into the frame, or if it can be 'wiggled' in the enclosure, then shims should be installed to take up the slack. Most strikes include shims and designate their installation locations without causing interference to the strike's action. The aim of shimming the strike is to give it a solid mount with the frame, not compensate for alignment issues. If those conditions are noted, then we recommend checking the squareness of the frame and alignment of the door.

*Final Function Checks:* At this point, the installer should check the strike's alignment with lock. Visually confirming the latches of the door lock are enclosed by the keeper is key. If the door latches do not physically make contact with any part of the strike when the door is shut, then the strike has been properly installed.



The goal of the installation is a strike flush mounted to the frame with no backpressure on the door's latches. If these situations are noted, they should be corrected before calling the job finished.

### Final Thoughts

Most of strike installation is unglorious and even rough, but doing the basic prep work is necessary for trouble-free use. If the installer does a thorough job on the 98% preparation work, then actually installing the strike is an easy 2% effort.

## Access Control Request to Exit (RTE)

For access controlled doors, especially those with maglocks, 'Request to Exit', or 'RTE' devices are required to override electrified locks to guarantee free egress.



We examine these key RTE factors:

- The Common RTE Devices: REX and Push Buttons
- Why Exit Devices Have Crucial RTE Importance
- Less Common RTE like Pressure Pads and Combo Devices
- Which Codes Cite Mandatory RTE Use
- Why Fire Pulls Are Not RTE, But Why They Function The Same

### Life Safety is King

Even locked doors need to unlock and allow egress. Life/Safety codes require it, with major code groups like [IBC \(International Building Codes\)](#) and [NFPA \(National Fire Protection Association\)](#) making them mandatory in most [building occupancies](#). In the final section, we detail relevant codes further.

## Exit Devices

For '[panic bars](#)', RTE is required on doors using maglocks and 'fail safe' bolts so they are unlocked when the exit device is activated to unlatch the door on demand for any reason.

Achieving this integration is required by code, cited in an IBC section named '*Electromagnetically Locked Egress Doors*' ([IBC 2015: 1010.1.9.9; IBC 2012 and 2009: 1008.1.9.9](#)). In summary, in [Occupancy Groups A, B, E, I-1, I-2, I-4, M, R-1 or R-2](#), buildings that use electromagnetic (maglocks) locks on egress doors equipped with exit devices **must have a built-in RTE switch** that releases the electromagnetic lock.

This is achieved by using an exit device with an integrated switch operated as the bar is pressed. A device mounted switch is often connected to the maglock and lock power via a door loop, or external wiring harness between the maglock and the exit device.



However, not all access locks need RTE in order to guarantee egress, which is why the code specifically targets maglocks. Example locks *not* needing RTE, per code, are electric strikes and latchbolts, because those types are typically mechanically overridden or latch retracted by door mounted exit devices. Free egress is maintained regardless of the powered security state of hardware, and so traditional panic hardware satisfies egress code requirements.

Even then, RTE sensors and switches may benefit access systems by providing an input to mute ambiguous 'forced door' alarms since no other system sensors can detect users leaving from the egress side of the door.

## Common Types of RTE Devices

When RTE is required, there are several types of devices that can be used to meet code.



Often, local AHJs will require more than one type of RTE per opening based on interpretation.

In the section below, we detail each major type of device or sensor:

- RTE PIR (often called 'REX' sensors, for 'Request to EXit')
- Push Buttons

We also examine several uncommon types of RTE for access, including:

- Pressure Pads
- RTE Integrated Devices
- Fire Alarm Pulls (That are not truly RTE, but work the same way)

### Motion Sensors (REX) PIRs

Commonly used as 'motion sensors' in intrusion alarm systems, 'passive infrared' RTE detectors are also mounted above doors to detect those approaching it for exiting.

When triggered, power to maglocks is dropped with no human intervention, so the 'no special tools or training' code requirement of the code is satisfied.

While any PIR can be used for RTE purposes, specialty RTE PIRs are built with a detection range limited to the area immediately in front of a door rather than the large area used in intrusion detection. For more on integrator nominated 'favorite' REX, see [Favorite Request-to-Exit \(RTE\) Manufacturers](#).



However, when REX/PIRs are used, additional RTE devices should also be installed, due to the fear of rising smoke potentially obscuring the sensor in a fire. Installing another form of RTE, primarily pushbuttons, allows for a 'manual' override should the PIR malfunction.

Using REX/PIRs is not without security risks, either. If a sensor is mounted incorrectly, it may actually sense movement on the wrong side of an opening, and they can be 'tricked' to unlock maglocks through a simple piece of cardboard slid under a door. For more details on that risk, see our "[Risky PIRs?](#)" report. Installers and maintainers should periodically check REX/PIRs for proper function and alignment during the course of use.

PIR RTEs typically range in price between \$20 and \$35 USD (including the top 'favorites' mentioned by integrators in our [Favorite Request-to-Exit \(RTE\) Manufacturers 2018](#) statistics), however higher end models ranging ~\$80 USD or higher may be specified for [explosion-proof areas](#), dual technology sensors to minimize false alarm potential or specialty units with [beam patterns customized for irregular openings](#).

## Push Buttons

According to code, these buttons have two main purposes:

- Interrupt lock operation/power for a timed duration, often 30 seconds
- Be clearly labeled as 'Press To Exit' as a door lock release, and be easily seen/illuminated

Often these buttons are used mechanically interrupt power to maglocks or other hardware. These buttons typically feature a mechanical or pneumatic timer so that power remains interrupted for a timed duration independent of access controllers or locks themselves.



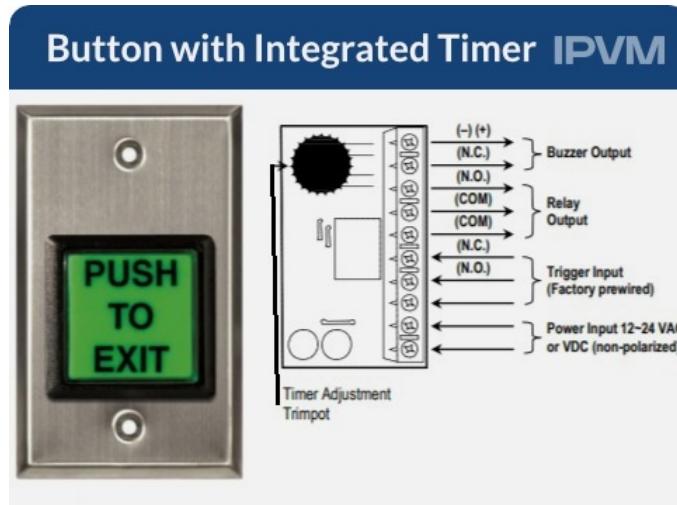
Code requirements do not always define the shape, size, color, or design of the button, but often defines the marking on the button and the height/distance from the door it must be hung.

In most English-speaking regions, the face or button clearly labeled 'PRESS TO EXIT' meets code, but local code exceptions and non-English regions may require an alternative/predominant language be used. In some areas, local codes may require bilingual labels used. The local code authority or AHJ will have clear direction on which language should be used if exceptions exist.

The timing function of RTE pushbuttons is generally accomplished by either of two methods:

- **Electric:** This type of button features a low-voltage or battery powered electronic logic timer that ensures a configured period expires before restoring power to locks.
- **Pneumatic:** These button feature a plunger and an air-powered piston that retracts at a slow interval. The RTE buttons require no outside power source or air supply for function, and generally are configurable for the same periods as the electric versions.

In order to satisfy the strictest interpretations of code, RTE pushbuttons often rely on an internal timer to break contact in a NC 'normally closed' power circuit instead of using a door controller's internal input contacts. Models with an internal relay are similar to the model below:



In terms of which type to use; electric buttons are more common and less expensive than pneumatic types. However, some AHJs and local code exceptions forbid electric type as potentially prone to malfunction, where pneumatic types are viewed as more reliable. However, because that preference is not defined by code, either type can generally be used.

Electric push buttons range in price between \$15 and \$35 each, with Pneumatics generally costing more, in the range of \$20 - \$50.

### Pressure Pads

A less common RTE device is a pressure pad, typically a mat placed in front of an opening that is designed to break power to locks when a human stands directly over it.

These pads are generally composed of a stiff rubberized, foam filled mat that makes electrical contact when weight presses the top surface to the lower surface.



A drawback of the pads is that they can actually become a nuisance or hazard if simply laid in front of a door, a problem typically resolved by installing them under carpets or flooring. However, while installing them below the floor keeps them from being kicked or inadvertently becoming door props, it also greatly inhibits maintenance and troubleshooting.

In addition, while pressure pads are reliable and can last many years of heavy use, they are expensive, with standard sized pads costing more than \$500 for a single door.

Unless RTE must be used in an area where hand contact or PIRs are not permitted, such as 'clean rooms' or [hazardous areas](#), pressure pads are not commonly used as RTE.

### Devices Factory Integrated With RTE

In order to simplify install and configuration of egress RTE, some access devices include motion sensor REX as factory-installed features.

A common example is where a maglock contains a pre-configured PIR onboard to interrupt locking when triggered:

## Maglock Integrated REX RTE

IPVM

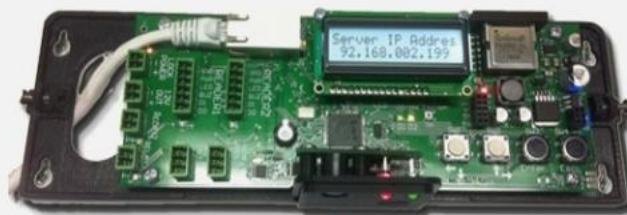


Maglock with integrated REX PIR motion sensor RTE

Another example is a door controller equipped with a similar PIR that automatically triggers the onboard relay to unsecure the connected lock:

## Controller Integrated REX RTE

IPVM



Controller Mounted Motion Sensor / PIR

While an integrated device can save labor hours in installation, they may invariably cost more and if the RTE device/sensor breaks, it may impact the security of the door in being replaced or needing service.



## Fire Alarm Pulls

While not technically an RTE device, if a facility has a fire alarm it must similarly be configured to drop lock power when the fire alarm is pulled.

Most maglocks and access control systems feature contacts to tie in the fire alarm, and AHJs require proof of successful maglock override by the fire pulls.

In no situation do fire pulls substitute for RTE hardware, however they should be installed to function in the same way.

## Code Basis For RTE

RTE need and installation is mandated in several 'model' codes, and often in multiple sections.

The major citation in access control are listed below:

- IBC: 'Door Operations' (2015: 1010.1.9; 2012, 2009: 1008.1.9; 2006, 2003: 1008.1.8)
- IBC: 'Sensor Release of Electrically Locked Egress Doors' (2015: 1010.1.9.8; 2012: 1008.1.9.8; 2009: 1008.1.4.4; 2006, 2003: 1008.1.3.4)
- IBC: 'Electromagnetically Locked Egress Doors' (2015: 1010.1.9.9; 2012: 1008.1.9.9; 2009: 1008.1.9.8)
- NFPA 101: 'Electrically Controlled Egress Doors' (2015, 2012: 7.2.1.5.6; 2009: 7.2.1.5.5)
- NFPA 101: 'Releasing Devices' (2015, 2012: 7.2.1.5.10-12; 2009, 2006, 2003: 7.2.1.5.9 - 7.2.1.5.11)
- NFPA 101: 'Access Controlled Egress Doors' (7.2.1.6.2)

For access to these model codes, see our: [Free Online NFPA, IBC, and ADA Codes and Standards](#).

## Exit Devices

Exit Devices, also called 'Panic Bars' or 'Crash Bars' are required by safety codes the world over, and become integral parts of electronic access control systems.



However, they are often poorly understood, especially how they should be used in electronic access control systems.

We explain:

- Where Exit Devices Must Be Used Per Code
- What The Major Components Are
- Why Mullions Or Vertical Rods Are Needed
- Why Electronic Latch Retraction Is Useful For Access Control
- How Power Is Routed To Exit Devices

### Mandatory Use

The application of exit devices is determined during building design by codes. Depending on [occupancy classification](#), openings are required to meet specific criteria related to their

opening during a 'panic' or emergency situation. Many code passages through IBC and NFPA relate to this subject, but the sections below provide the basic performance requirements of this hardware:

**NFPA 101 : 7.2.1.5.9 - 7.2.1.5.11, 2015:**

Latches or other fastening device on a door shall be provided **with a releasing device having an obvious method of operation under all lighting conditions**. The releasing mechanism (except existing installations) shall be located between 34" and 48" above the finished floor. Doors shall be openable **with not more than 1 releasing operation**:

- each leaf of a pair in a means of egress shall have its own releasing device, and **each device has to operate independently (can not require 1 device to be released before the other)**, except
- no additional locking device (padlock, hasp, chain, deadbolt, etc.) shall be installed on a door which requires panic hardware

Exit devices are not specifically identified in codes as the only solution for these openings, however, the design of modern panic hardware typically represents the least expensive and most reliable products marketed to be code compliant.

'Paddle devices' are an alternative but may not be compatible with the door leaf or be code compliant according to local interpretations (ie: usable in 'all lighting conditions')

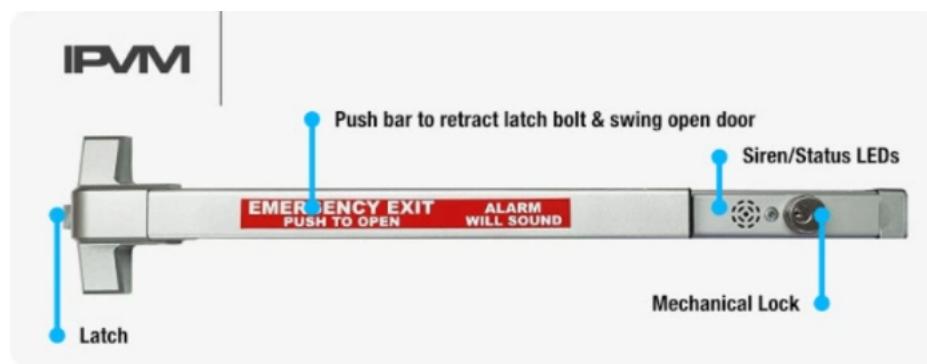
In general, exit devices are required in any facility where:

- medium/large groups congregate: (halls, public buildings, daycares, hospitals)
- where commerce to the public is performed (commercial/retail properties)
- where risk requires evacuation plans (most commercial/industrial classifications)
- where large quantities of materials are stored (warehouses, storage facilities)

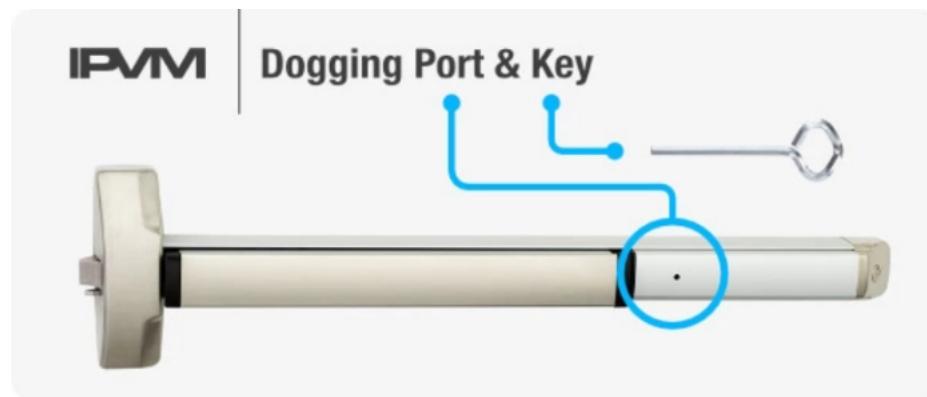
This criterion covers the majority of non-residential properties.

## Major Exit Device Components

While large, bulky, and potentially mechanically complex, the operation of an exit device is simple: Push the bar, retract the latch, and swing open a door. The basic design of exit devices are shown below:



In addition to the above features, the ability to 'dog down' a device, or lock the bar/latch into an unsecured position, is a common feature. Typically, this function uses a common hex key to lock a device open.



Exit Devices are complex devices because of the '*not more than 1 releasing operation*' code requirement that often means the locked latches must be retracted in multiple locations in multiple directions with one motion. Exit devices often include mechanical linkages and are sensitive to adjustments and orientation with the door frame.

While the 'secured side' configuration of an exit device is similar regardless of unit, the 'outside' or 'unsecured' side of a device is subject to wide configuration. In many cases, a simple door handle is used, but 'outside key access' that allows an outside lock to unlock the door from the unsecured side is used.

### Latch Location

The location of the latch is a critical feature, especially when exit devices must work with EAC systems.



The latch is important because it is the physical component that secures the door. With exit devices, there are typically three different latch locations, with a single device controlling up to three latches simultaneously.

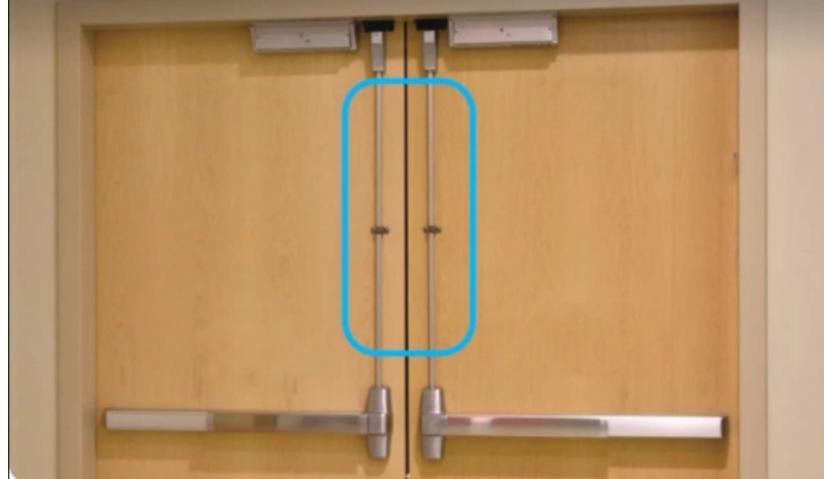
### Mullions Or Vertical Rods

In large occupancies, double doors are common because they permit more people to enter or leave than a single door. As such, exit devices are often found on double doors. In many cases, the omission of a center post, called a mullion, changes the latch position. When the mullion is present, latches are generally contained in the 'device head'. However, when the mullion is missing, the door must be secured into the top or bottom of the door opening.

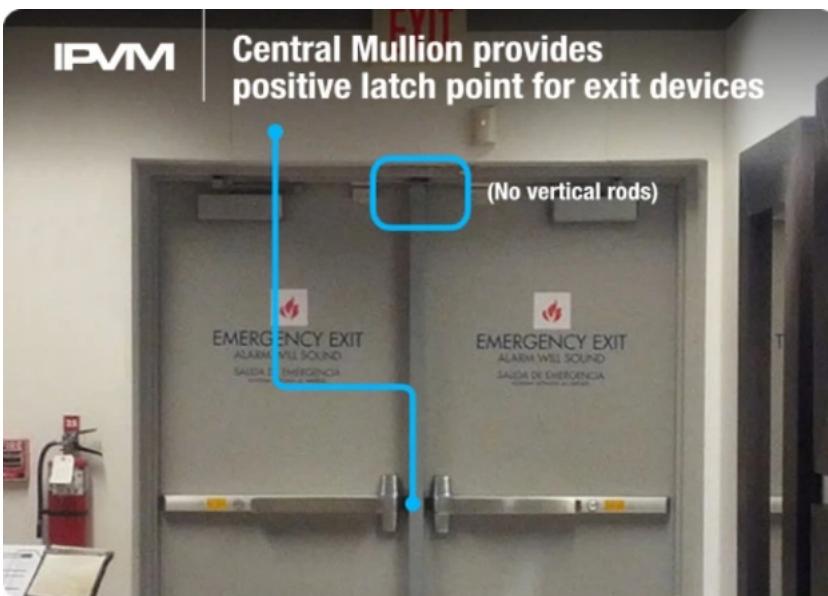
Devices with no mullion use rods:

**IPVM**

**With no central mullion, doors  
'lock' into top frame via vertical rods**



Devices with mullion latch without rods:



Because the latch location changes, this affects the way the door interfaces with an access system. For example, it may affect the selection of an electric strike to be a top-frame mounted double vertical rod strike. Or the location of the vertical rods may complicate the mounting location of a maglock. In either case, the selection of electrified locking hardware is affected by the type of exit device hung on the door.

## **Electronic Latch Retraction**

Another option is to apply 'electronic latch retraction' to the device. This powered feature acts on the latch as if the bar was being pushed when a credential is read. This allows an exit device to remain 'undogged', but opened from the outside regardless of what is happening on the inside of the door:



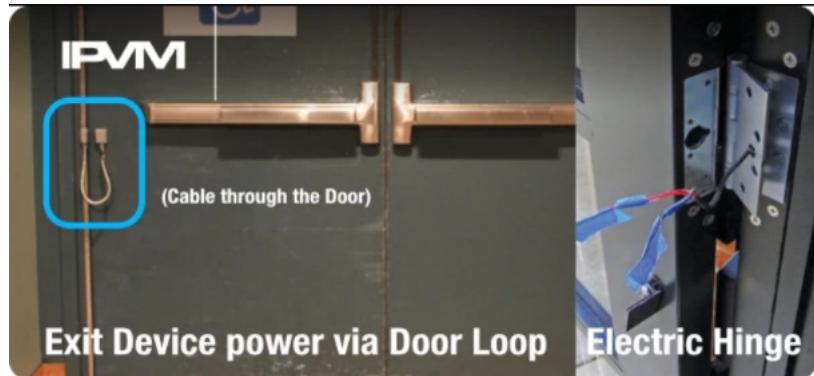
Even when the device is not initially specified with this feature, retrofit kits are available from many manufacturers to convert units.

When used with EAC, the exit device interfaces with the controller like a strike - generally the unit is unpowered until a credential read causes the system to apply power to the retraction mechanism. Regardless of the type of latches used - concealed/surface rods or strike latches, variations on electric latch mechanisms are available.

## **Getting Power To Devices**

When exit devices need electricity, powering them can be a challenge. Unlike other electric locks that are powered by cabling run through the frame, exit devices hang on and must swing with, the door leaf.

Usually, cabling for latch retraction and other electrified features is run to the device in one of two ways: Door Loops or Electric Hinges:



Electric (or Powered) Hinges are not motorized or mechanically different than standard hinges, they simply are constructed to pass-through power from one hinge to the other with internal pivoting contacts. Because the door (often) swings on hinges, the reliability and safety of these conductors are critical. Unfortunately, power hinges often wear and break over many years, and the equipment may need to be periodically replaced.

Another constraint of electric hinges is that they must be run inside 'hollow core' doors. While running power internally to the door is safer and more secure from tampering risk, it excludes 'solid core' doors unless additional core raceway drilling [link no longer available] is performed.

In this situation, a 'door loop' is used, which is essentially an externally run cable, usually in some form of a flexible armored conduit. The loop is run on the secured (inside) of the door, and externally vandalism is not generally an issue, but internal tampering and damage can be.

Other common features requiring power in exit devices are:

- *Sirens*: Devices are available that emit an alarm when the bar is pushed and the door opens. This is a useful feature for 'emergency exits' that are not 'normal' passages. When someone opens the door, the alarm attracts attention.
- *Delayed Egress*: In some cases, the door can be kept locked for a short period of time before opening. Local codes heavily legislate the acceptable use of delayed egress, but in all cases, a siren must sound during a delayed period. As we cover in our '[Delayed](#)

[Egress Tutorial](#)' report, this is a useful feature to keep people secured for a short period of time while still allowing emergency exiting.

### **Relative Cost**

The price range for an exit device ranges wildly, from under \$500 economy grade devices to \$4,000 heavy-duty, architecturally styled units. In general, the retrofit retraction kits cost around \$400, and other locking hardware like strikes or maglocks fall in line with typical pricing, from \$100 to \$700 depending on style and holding power.

### **Other Details**

Most of the time when installing EAC on exit device doors, the actual devices have already been specified, installed, and in use. However, other constraints factor when specifying new exit devices on doors, namely UL rating and door type (glass, wood, or metal).

## Door Closers

Door Closers have an important job: automatically shut doors when they are opened, because an open door cannot control access.



We review Door Closers, examine how they are selected, and how to avoid misusing them:

- Why closers are important for access control
- Why using closers as barricade locks is often illegal
- Applications other than security where closers help
- What normal closer operation should look like
- The 3 standard movement phases and configuring locks for them
- How to properly size closers
- Typical closer pricing

Finally, the 6 question quiz at the end will test your knowledge.

### Crucial Security Role

Closers address a fundamental access problem: doors must be closed before they can be locked.

Unless people are in the habit of pulling every door behind them, there is no guarantee it is closed unless these devices are used. Since basic access control requires keeping unauthorised people out of areas they do not belong, an open door simply offers no security to the people or assets inside.



Simply: Closers are designed to shut doors behind every user so relocking can automatically take place, mitigating the risk of an open door allowing anyone free access into an area.

### **Illegal Use As Barricade Locks**

A recent trend in classroom barricade locks involves for using a metal sleeve that fits over the closer's arms when closed, preventing further opening of the door with the unit in place. These devices must be installed with the door closed, and tout they protect teachers or students from dangers in hallways when fitted:



However, these devices are often illegal because they risk trapping occupants behind barricaded doors when exit might be crucial. Most local authorities have adopted codes that dictate emergency egress is a simple, instinctual action.

The model code for most of these local regulations is International Building Code (2018) 1008.1.9 that states:

"Except as specifically permitted by this section egress doors shall be readily openable from the egress side without the use of a key or special knowledge or effort."

Bottom line: any piece of security door hardware must also guarantee safety, and closer barricade locks are risky for protecting lives as much as keeping them safe. We examine closer barricade locks further in [Classroom Closer Lock Illegal note](#).

### **Other Benefit For Installing Door Closers**

However, security is not the only benefit closers provide. They are often designed into a facility for other reasons, including:

- *HVAC Efficiency*: Keeping air handlers balanced and minimizing conditioning cost requires keeping zones sealed. To avoid circumstances like an conditioned office from being heated/cooled by an adjacent warehouse space, door closers are used to keep the zones separate.
- *Noise Isolation*: Likewise, a closed door offers some noise isolation. Closers help keep quiet areas quiet by keeping doors shut.
- *Fire Protection*: With so much emphasis on 'positive latching' of locks to keep firedoors closed, closing the firedoor first is a huge factor in enabling the firewall to do its job. AHJ approved Fire Door closers automatically shut open firedoors during an emergency, typically triggered by the fire alarm.

## Hydraulic Closers Are Most Popular

Most modern closers are a 'hydraulic' (oil filled) box that are surface mounted on the secured side of the door. In order to prevent occupant injury, closers have 'stages' using different timing and closing force as the door is shut.

In the gif below, a hydraulic closer displays the three different stages of closing in one fluid movement:



[Click here to view the animated gif on IPVM](#)

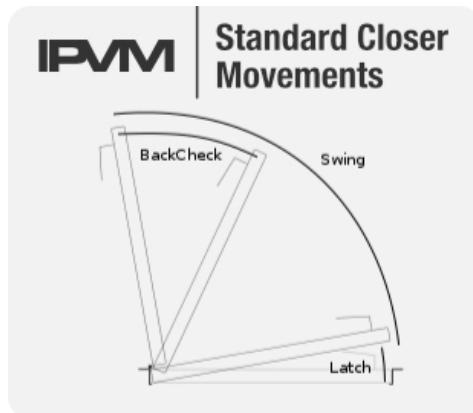
The importance of these positions are noted and explained in the following section.

## Standard Movement Positions

The three typical phases are shown in the top-view door image below:

1. *Back Check*: This phase is similar to an 'over-travel' that allows the door to open fully, even beyond 90 degrees, so that wide loads can pass through. The back check phase typically places the closer at a mechanical disadvantage and requires more directional force at a leverage disadvantage, without damaging the door or the closer.
2. *Swing*: This is the 'primary' phase of the closer, that swings the door closed. A variety of closers match the door, taking variables like [Door Handing / Swing Direction](#) and duty cycle into account.
3. *Latch*: The last, most subtle stage may be the most important: 'latching' slows the swing action down and makes the movement much more stable and rigid so the

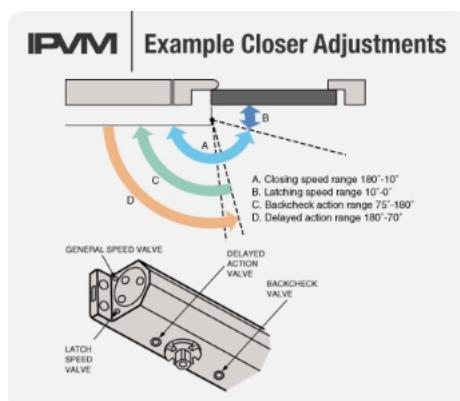
accompanying door locks can reliably relatch. Instead of a door slamming shut and bouncing off the frame, the latch phase is a controlled close.



When in the 'latch' phase, locks should be adjusted to accommodate for delayed unlock or relock times if needed, and while the overall operation of a close can take 45 seconds, the 'latch' phase alone may account for 5 - 7 seconds despite only moving a few inches.

### Timing Adjustment Critical For Access Control

Fortunately for access systems, modern adjustable closers typically have multiple screws that tweak timing or free travel when they are tightened or loosened. The exact location and number of adjustment points vary, but they generally are found on the underside of the unit and can be adjusted with small standard hex keys or allen wrenches:



A closer is properly adjusted when there is no slamming and reliable positive latching of all companion locks. Usually spending ten or fifteen minutes adjusting a closer after three to five years of use is needed, but it may be critical for getting the door to work with electronic access control properly.

### **Other Uncommon Closer Types**

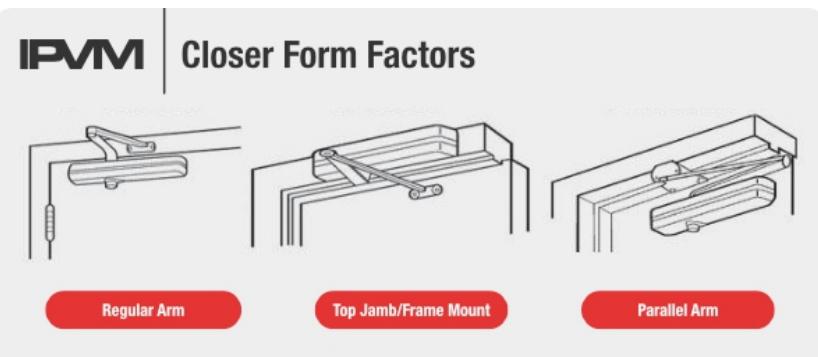
While hydraulic closers are the most common, there are many different types used in a number of applications:

- *Electromechanical*: When combined with Door Holders (devices that keep doors open), electro-mechanical devices are often used that pair maglock holders with door closers in an electrified unit.
- *Full Concealed/Specialty*: Where architectural design and aesthetics matter, closers that can be hidden inside doors, frames, or hinges/pivots are often used. Unlike other types, these are often matched and installed at the factory and may not be field serviceable using conventional components.
- *Pneumatics*: In hazardous or contaminate-sensitive environments, hydraulic closers may not be permitted. While uncommon in commercial openings, air-powered closers (often with accompanying compressor units) are used to eliminate the risk of oil-based units.

### **Sizes Based On Closer Form Factor and Door Width**

Most access jobs will not require installing new door closers, however replacing worn or broken ones may be fairly common. Additionally, installing new closers on doors previously prone to be left open can tighten up access in vulnerable areas.

For access installers ordering replacement retrofit units, noting the current type of closer and how wide the door dimension it is attached provide the right information for ordering new closers. The three basic closer form factors are:



The right type to use is typically limited by [Door Swing](#) and by the aesthetic appearance of the devices. In general, Regular or Top Jamb units are used unless the way their arms project are considered obtrusive. In that case, Parallel Arm types are used as long as the door width is not over 42".

The strength of the closer is determined by standard 'size', also called 'spring size' despite also applying to oil-filled, springless hydraulic units. In general, the greater the 'size' number, the stronger and physically larger the unit is when mounted onto the opening:

DOOR CLOSER SELECTION CHART	
Door Width	Min Closer Size Needed
Less than/to 30"	#3
30"- 36"	#4
36"- 42"	#5
Widths more than 42", use #6 regular/top jamb closers only (too wide for parallel)	

While often preferred for their flush arm action, Parallel Arm closers are often too mechanically weak to close doors wider than 42", and other action types with more mechanical strength must be used.

## **Closer Cost**

In most cases, Regular/Tom Jamb adjustable hydraulic closers should be installed for access control, the other types are too uncommon, too application specific, or too inflexible to be retrofitted to existing doors.

Not only can they be specified to fit most openings, but installing them can be done with basic tools, the units can be tweaked for the specific opening, and for most common door widths using #3 or #4 size units, pricing less than \$300 - \$350 from security distributors.

For wide doors, closers sized #5 - #6, the cost is ~\$450. For very wide or atypically sized openings, units can be priced ~\$2,000 or more and specialty training to install and adjust may be required.

Door dimensions, door weight, hinge type, and expected uses per hour all play a key role in selecting the right unit. Most closer manufacturers provide a specification guide to help zero in on the recommended unit.

## **Quiz Yourself**

Take the six question [Door Closers For Access Control quiz](#) now.

# Door Operators

Doors equipped with door operators, specialty devices that automate opening and closing, tend to be quite complex.



The mechanisms needed to achieve these actions, the configuration how they work, and how they integrate with standard access systems can be hard to get right.

We examine:

- Purpose of door operators
- Swinging vs sliding vs revolving door operators
- Wheelchair access doors
- Low energy ratings
- Pricing of operators
- Integrating access control - Activate Buttons or Direct Operators

## Purpose of Door Operators

The simple action of opening and closing doors takes one of the most high-tech devices to accomplish. Given the physics behind swinging or sliding a door, operators must be strong, precise, reliable, and safe.

Unlike 'dumb' [Door Closers](#) that typically just use hydraulics or pneumatics to shut doors, Operators are almost always 'smart' electrical devices that include mechanical components and intelligent controllers that coordinate movement in multiple door directions and must sense when to stop so they do not injure users.

### Designs Vary Based On Door

While the actual components vary by design, most operators consist of multiple machined assemblies, motors, belts, levers, cylinders, and carriages. A typical 'slider' operator cutaway is shown below:



In many cases, the operator is designed to work a specific opening, and the entire door/frame/operator is designed and installed as a single assembly.

The type of door dictates the type of operator used. The major types used in commercial, industrial, and public buildings are:

- *Swinging*: For doors that open in/out on pivots or hinges, swinging operators handle movement of the door leaf. Most handicap/wheelchair access doors use this type of operator.

- *Sliders*: Especially for high-volume openings, like those used for big box retail or supermarkets, sliding operators are used for their fast speed and ability to move big sections that support heavy traffic.
- *Revolving*: Where security or environmental controls are important, revolving doors are used to control entry and egress in spaces, often in high-end commercial spaces or high-security installations.

## Wheelchair Access Doors

The most common application for operators in commercial buildings is door automation for those with accessibility issues or wheelchair access. In general, a user does not need strength or ambulatory movement to open and close the door equipped with an operator, it is typically push-button activated. While comprehensively [defined by ADA](#), in countries where ADA is not formally adopted, the design guidelines are still typically used.

The general process is shown below:

[Click here to view the Wheelchair Access – Storefront video on IPVM](#)

For high-security facilities controlling access, the mandate to have accessible doors but keep them locked is tricky for integrating access control.

Notice the user activates the door by button (it is not automatic), and the door is timed to stay open and slowly close to allow the users to wheel through. The entire process, from buttons used, fully automatic operation (no button needed), to opening/closing force, cycle time, to additional safety gear like handrails and signage is heavily legislated by codes. We examine this in detail below.

## Low Energy Ratings Explained

The term 'low energy' operator only applies to swing action types, and has nothing to do with input power or voltages. Rather, the 'low energy' designation pertains to the force required to push the door open as an assist device.

According to ADA, the maximum operable force for door hardware is 22.2 N (5 ft/lb). In countries where ADA is not formally adopted, the design guidelines are still typically used. Because this rating is so slight, most existing [Exit Devices](#) do not meet the criteria, and so a designated opening is fitted as a wheelchair accessible opening to meet code.

In order to achieve the 'low energy' certification mandated in code, the operator must be limited in two parameters according to [ANSI A156.19](#):

- *Imparted Force*: No more than 15 foot pounds of force at the sweeping edge of the door, to avoid crashing into people or knocking them off-balance.
- *Opening Speed*: No faster than 3 seconds to fully open, remain open for no less than 5 seconds, and close no faster than 5 seconds.

Additional requirements are the initiation of action must happen by button push (not automatically by motion sensor) and in event of power failure cannot require more than 30 foot pounds to manually open.

When these conditions are met, the safety device requirements are greatly reduced, and expensive/cumbersome adds like safety handrails, motion canceling scanners, and pressure mats are not required as they are with 'high energy' swing operators.

Notice in the image below the reader is positioned behind the door, but the activating push button to operate the door is well clear of the door swing. In this example, a wheelchair user scans a credential at the reader to active the button, then must roll backwards to depress the button to automatically open the door in a location where the door swinging action will not hit or trap the user behind it:



If the operator was triggered directly by the reader, the user could be crushed by the swinging door. As installed, however, a wheelchair user is significantly disadvantaged by scanning then switching direction in order to push the button.

### Sliding Doors

Most common in retail stores or buildings where high volumes of people are entering/exiting, sliding doors are used because they move quietly, rapidly, and most often automatically:

[Click here to view the video on IPVM](#)

In general, sliders are high-maintenance openings and require frequent adjustment and can wear rapidly based on heavy use. These operators and openings are typically installed and serviced by specialty contractors (like [Stanley](#)) and integration to access control often requires joint cooperation among vendors.

### Swing Doors

For traditional swinging doors, operators that move door leafs on hinges or pivots are used. In the example below, notice users are automatically sensed by motion sensor and do not need to press buttons to activate the door.

Unlike a wheelchair door, this is a 'high energy' operator that requires additional safety equipment like handrails to be installed:

[Click here to view the video on IPVM](#)

### **Revolving Doors**

The most elaborate, expensive, yet 'high security' operator is attached to revolving doors. Similar to [turnstiles](#), revolving doors only allow one or a few people in at a time and keep internal environments separated from outdoors. Operators keep the door segments moving at a slow rate, but can detect and stop movement when they contact a stationary or slower moving object like a dropped bag.

This type of operator is often used in architecturally significant or 'grand' entries for large skyscrapers or convention centers:

[Click here to view the video on IPVM](#)

### **Operator Prices**

In general, operators are expensive and require the entire opening to be matched. In most cases, the frames and doors themselves are also included or must be replaced, greatly increasing the cost and labor required. In terms of operator cost alone, most commercial grade [low energy swing operators](#) cost ~\$1,000- \$2,500, while a high energy or sliding type can be 4x or 5x more.

In general, the cost of the operator is a fraction of the entire bill of material to fully outfit a door, and installation and service typically requires dealer relationships with manufacturers who may require factoring training installers before resellers are approved to do business.

## Integrating Access Control

There are two major methods of integrating operators with access systems. In both cases, readers are connected to access controllers that:

- *Activate Door Operators:* Impulses from the access system directly trigger a door to open.
- *Activate Push Buttons:* The access system activates the pushbutton, which allows the door to open when pressed.

In terms of which option to use, available inputs on operator controllers and the presence of push buttons, compared with the availability and location of output contacts on door controllers impact which one is best.

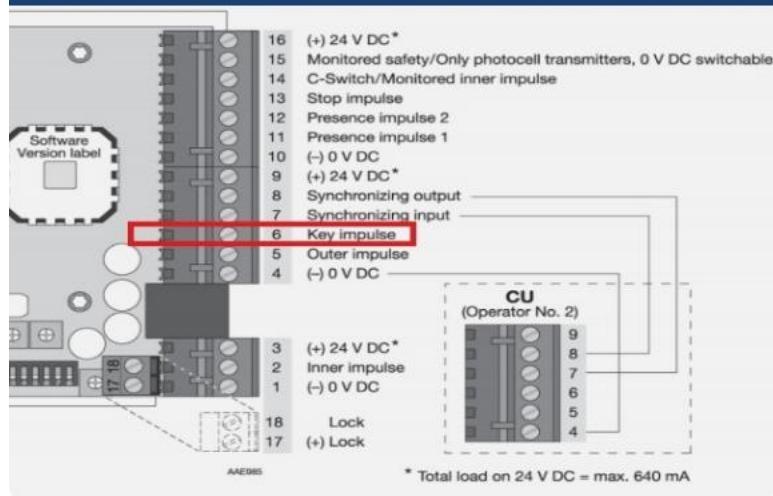
In the picture below, the circled reader triggers the door cycle directly:



This integration must be supported by availability of an open input contact on the operator, usually called a 'Key Impulse' or similar to the [connection diagram shown for the operator below](#):

## Example Controller Connection For Operators

IPVM



The other method of integration relies on activating the push button when a valid card is read, which otherwise means the button is unpowered and nonfunctional. In many cases, this method is used when the door is scheduled open for a long period during the day, but access controlled on schedule at night or on the weekends. This method requires that push buttons are present, but eliminates the need to directly integrate to an operator. The images below show such installations:

The reader above the push button:



And a system where either a dedicated magstripe or general contactless access credential 'unlock' a button:



### Broad Access System Support

In general, any access system with controllers that include a conditionally linked output can be used to control an operator. Most major commercial and enterprise access platforms include this while 'starter' systems designed for smaller door counts and more basic applications may not, especially 'combo' alarm panel based systems.

## Door Position Switches (DPS)

Door position switches are frequently ignored or forgotten, yet can solve major access control problems.



Access 'control' itself relies on these switches to make the right logical decisions about sending alarms and locking doors. We look at how to choose the right set of contacts for your door and cover these details:

- Sensor Function
- DPS Importance
- Sensor Types Available
- Doors Impact Selection
- Common Sensor Types
- Common Sensor Mount Locations
- Sensor Pricing
- Controller Connection Location
- Mitigating Magnetic Tampering Risks

## **Door Position Switch Function Overview**

For access control, 'door position switches', also called 'DPS', 'door monitors', or 'door sensors', detect whether a door is opened or closed.

Typically the access control system controller or door interface module is where this sensor is connected. The method of sensing is simple: when a door is shut, the circuit is complete. However, when the door opens, the circuit breaks open, signaling to the access system the door is not closed. Since doors cannot be locked or 'secured' when opened, this sensor describes where a facility is most vulnerable.

### **Security Important, But Often Ignored**

Access control systems are blind to whether a door is open or shut without position switches. Because open doors cannot limit entrance or prevent unauthorized people from entering an area, DPS is the primary way the system 'knows' whether or not a door is secure.

Many installers do not install DPS in order to 'save costs' or otherwise consider DPS optional, but this omission is a critical mistake. Without DPS, access control cannot be verified 'controlled' at all, and installing DPS should be a mandatory aspect of every opening.

### **Broad Selection**

Because door position switched are used in a variety of systems, there are thousands of options available. Among those thousands, there are five or six basic types used in electronic access:



Many installers use the 'magnetic' bullet types in every situation and struggle with seemingly sporadic false alarms and system trouble ever after. Like other access components, choosing the right door position switch depends significantly on the door - which type of door it is, how often it is used, and even which direction it faces. We address these factors in detail below.

### The Opening Matters

Right or wrong, switch selection is typically based on familiarity, when they are installed at all. Some types of DPS switches are more difficult to install than others depending on the door itself.

For example, if a door frame is installed into a solid concrete or masonry wall, drilling enough clearance and running wire to a "Plunger" frame style will be difficult. However, a "Magnetic" door-mounted type cannot be field installed into pane glass or Herculite doors.

Hollow metal steel doors may not easily be drilled to fit "Recessed" types, unlike traditional wood doors:

Contact Install Often Recessed Into Door **IPVM**



### Mounting Location

The next factor to consider is where the sensor should be installed. There are a number of standard locations to choose from, shown in the image below:



The type of opening once again influences this location. Aside from the physical type of door, how it is used and where its located play a key role, including:

- *Exterior/Interior*: What kind of environmental conditions is the sensor exposed to? An air-conditioned office, or an opening exposed to extreme weather?
- *Wind/Ice/Snow*: If the gaskets or thresholds around the door fail, will the sensor be exposed to moisture, mud, or grime?
- *Traffic Volumes*: How often is the door opened? Once per shift, or a hundred times per hour?

Taking a survey of the door and recording how it is used help define the best sensor type, attributes that we cover in the sections below:

## Magnetic 'Bullet' Style

This type of sensor is the most common, usually requiring the wired piece to be installed into the frame, and the solid 'magnet' piece being installed into a drilled hole in the door.

In most cases, this type of sensor is hung on the 'swing' side and is recessed during installation so tampering/detection is difficult.



- Pros: Magnet 'bullet' sensors are concealed and aesthetically accepted in most facilities. Installation is easy, requiring a minimum of drilling and wire run difficulty.
- Cons: Very prone to alignment issues. The detection range can be very precise, with sensors needing to be installed immediately adjacent to each other. Vulnerable to false alarms, especially if doors are buffeted by wind or vibrations.

## Plunger Style

A mechanical, not magnetic, style of sensor. When the door is shut, the leaf presses a button, completing the circuit. When the leaf opens, the button is released, signaling an open.

Because plungers are mechanical, they are not subject to false alarms caused by wind or vibration. Typically plunger DPSes are installed on the hinge side.



- Pros: Very durable, usually lasting millions of cycles. A 'one-sided' sensor that avoids alignment issues.
- Cons: Prone to sticking because of dirt/grime. Easy to tamper or defeat with a card or screwdriver unless protected by frame and jamb threshold.

## Surface Mount Style

Easy to install on most types of doors: wood, aluminum frames, and hollow-core steel. Alignment problems are somewhat mitigated with a larger sensor area.

- Pros: Rugged and generally resistant to negative environmental effects (heat/cold/rain/snow). Minimal installation skill required.
- Cons: Exposed and subject to vandalism. Potentially unattractive in architecturally sensitive doors.



## Recessed Style

A hinge side-mounted sensor, very useful on thin frame storefront glass openings. Generally, only one side is wired, which is run inside the frame side.

- Pros: Not prone to the tampering vulnerabilities of plunger types, and fully concealed.
- Cons: Generally more expensive and more difficult to install than Surface styles. Risk of damaging door or not having frame clearance could be undetected until trying to install them.



## Overhead Door

A specialty sensor designed for doors that separate 'up' rather than swing. Overhead/roll-up doors are difficult to monitor with traditional sensors, due to size and location of structural features.



- Pros: Easy to install, and generally equipped with a substantial armature and armored housing for heavy-duty use.
- Cons: Still susceptible to false alarms due to wind buffeting. Vulnerable to dirt, grime, and forklift damage.

## Sensor Price

The cost of DPS sensors is generally minor, with installation labor running higher than the price of the sensor itself. Most types are available for under \$10, with only 'high security' or ruggedized models being more expensive.

## System Connection Location

Door Position Switches are connected to the [Access Control Door Controller](#) usually in the set of contacts specifically labeled for 'DPS', or in the case of the controllers below, as general inputs that are configured for DPS use in configuration screens:

**Installed as Inputs on Controller**
IPVM

LP1501 Installation

**Input Circuit Wiring:**

Typically, these inputs are used to monitor door position, request to exit, or alarm contacts.

	Standard Supervised Circuit, Normally Open Contact
	Standard Supervised Circuit, Normally Closed Contact
	Unsupervised Circuit, Normally Closed Contact
	Unsupervised Circuit, Normally Open Contact

HID X100 Installation

**HID**™ Powering Trusted Identities      [HID Aero™ X100 Installation Guide](#)

**4. Input circuit wiring**

Inputs are typically used for the following:

- To monitor door position.
- Request to exit.
- Alarm contacts.

Unsupervised circuit IN 1 to IN 4

Usually, these inputs are simple 'normally closed' circuits, and field power is typically not issued by the controller for DPS use.

## Sensor Type Selection Guide

Based on the door type and installation location, guidelines for sensor type selection are:

- *Perimeter Doors*: Use Bullets or Recessed Magnetic styles, depending on the 'drillability' of the door.
- *Glass Doors/Thin Frames*: Use Surface Mount or Recessed styles depending on frame clearance and door frame mounting area.
- *Office/Corridor*: Use Bullets or Surface Mount styles, because the weather is not usually an issue and quick installation keeps the cost down.

## Common Drawbacks

DPSes are not without trouble, however. Many choose to sidestep potential performance issues by simply omitting them from designs, however, most manufacturers' support and best practices recommend their use. In general, when a sensor becomes a source of false alarms, one of the following situations is the culprit:

*Dirty/Sticky Contacts*: Magnetic or mechanical sensors are coated in grease, dirt, or floor wax so they cannot reliably break contact. A simple rag and light solvent wipe can fix the problem, but continual exposure may require frequent replacement.

*Misalignment*: Doors and frames move over time, through simple use. Sometimes the door shifts enough that realigning the door or tightening up the hinges may be required.

*Weather Damage*: Thermal exposure can cause magnets to become less sensitive over time, and greater issues of contact corrosion in some environments can prematurely end sensor life. Replacements may be required more frequently on exposed doors than others.

## Magnetic Tampering Risk

Non-mechanical sensors typically use magnets to sense open/close state. Because of this magnetic sensitivity, some sensors make it possible to 'fool' the sensor into staying in a 'closed state' if a more powerful, stronger magnet is placed adjacent to the sensor, even for sensors recessed into frames.

High-security sensors like [Magnasphere](#) can be used in place of standard DPS to harden an opening against the exploit, or using [Lock Status Monitoring](#) instead can avoid easy magnetic defeats entirely, although those options typically cost 30% - 50% more than conventional methods.

## Lock Status Monitoring

Just because access doors are closed does not mean they are locked.

Unless access systems are using lock status monitoring, the doors and areas they protect could be left insecure. How can you tell when doors are locked?



Lock status monitoring addresses a key vulnerability of many access control systems, but its value is commonly ignored or misunderstood. We explain:

- How Lock Status Monitoring Prevents Security Risks
- Why Shut Doors Do Not Mean Secure Doors
- Tradeoffs Of Door Position vs.or Lock Monitoring
- Typical Lock Monitoring Cost
- Examining Latchbolt Monitoring vs Latchbolt Strike Monitoring
- Explaining Maglock Bond Sensors

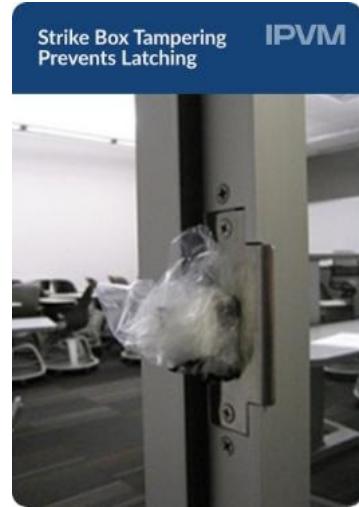
### The Importance Of Lock Monitoring

'Lock monitoring' checks to see whether an opening's hardware lock is reporting itself as locked.

Because most electrified locks can only secure openings properly when the door is shut, Lock Monitoring essentially notifies access systems that doors are both closed and secured.

### Monitoring Against Lock Tampering

Even with sophisticated electronic access locks, door hardware is vulnerable to tampering. Unless the lock hardware itself is monitored as being locked, tampering can defeat their strength and be undetected by the system.



For example, [electric strikes](#) can be neutralized by placing foreign objects in the strike so the latchbolt never fully engages, or held in with tape so they never extend at all. The image to the right shows how trash can be used to prevent the latch from extending into the strike to keep a door locked.

And while [maglocks](#) generate large amounts of holding force, it works only when the magnet and the armature have full contact.

The rated magnetic holding force drops drastically if their pieces are not allowed to contact each other, even just through covering the surface with tape or paper, dropping the bond from thousands of pounds to just a few hundred, allowing for doors to be easily kicked open.

The image below shows a strap of velcro used to interfere with a maglock's bond so the door can be opened even if the maglock is configured to be locked:



### Shut Doors Do Not Mean Secure

The scary part is that these doors may otherwise appear fully closed to an access system, but be significantly insecure and unlocked or weakly locked in reality. Even a door equipped with [Door Position Switches](#) can only tell access operators if a door is open or shut, leaving the assumption that 'closed' also means 'locked'.

Unfortunately, many attempts to defeat access controls come from insiders, often for convenience and not malice, as noted in our [Propped Doors Access Control Tutorial](#). However, even if done without criminal motivation, tampering with the access lock can leave free, uncontrolled entry through the door to employees or outsiders alike.

### Door Position Inputs Used For Lock Monitoring

In many cases, using lock monitoring costs moderately more than door position switches. For many access [Door Controllers](#), either Door Position Switches or Lock Monitors are connected at the 'Door Monitor' input, usually a simple Normal-Closed circuit on the controller board.

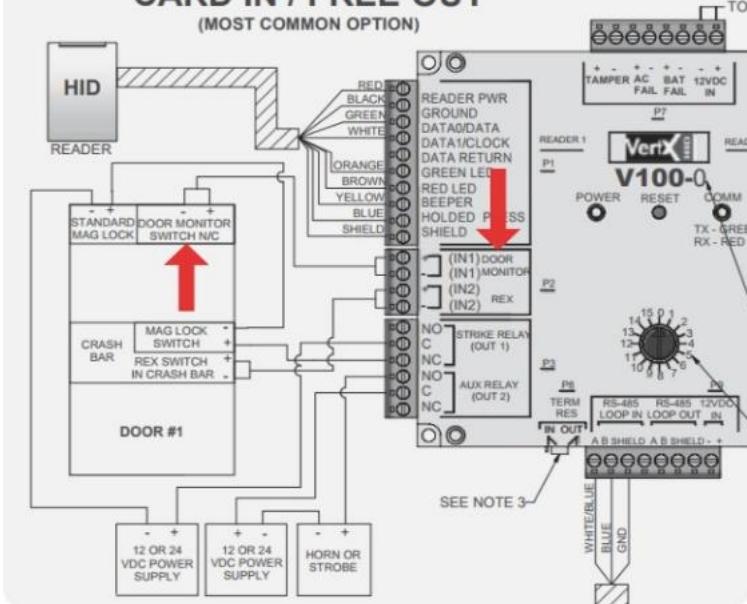
Here is an install wiring example for an HID controller:

## Door Position Switch Inputs Used For Lock Monitoring Too

IPVM

### V100 - DOOR/READER INTERFACE CARD IN / FREE OUT

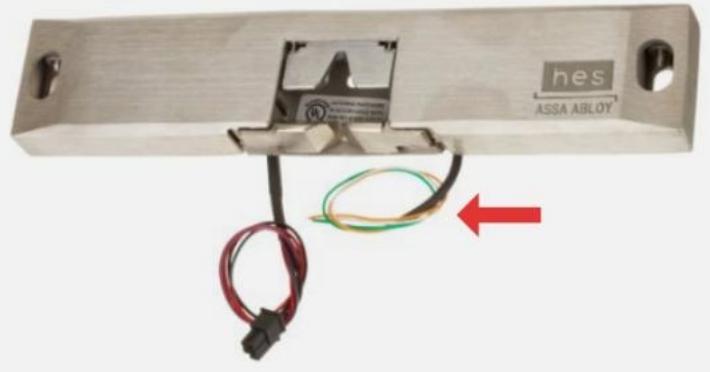
(MOST COMMON OPTION)



The cost of adding a surface-mount door contact can cost as little as \$5 per set, and with a few minutes of install, connected to an access system. However, specifying integrated lock monitoring in the lock itself can add 5% - 10%, often \$20 or \$30 to the item's cost. The cost difference may explain why lock monitoring is not as commonly used as Door Position Switches.

In the strike below, the integrated latch monitor is connected to controllers by way of the yellow and green wires:

## Latchbolt (LBM) Monitor Wire Leads Included **IPVM**



The wiring harness for these components in all types of locks (ie: strikes, maglocks, or electric latches) is often totally separate from power wires, and leaving latch monitoring unconnected generally still leaves the lock normally operational.

### Three Common Forms

Lock monitoring is usually deployed in three ways:

- Latchbolt Monitoring (LBM)
- Latchbolt Strike Monitoring (LBSM)
- Maglock Bond Sensors

While the first two seem to be labeled almost the same, the monitoring methods are drastically different. And even a lock with no moving parts, like a maglock, can be monitored by checking its bond strength. We examine the three methods below:

### Latchbolt Monitoring

One way to check if doors are closed and their latches engaged is by 'latchbolt monitoring'. In this method, a mechanical or inductive switch built inside the strike checks whether or not the door's latchbolt or deadbolt is extended. If the latch is thrown, the LBM pressed in. If the latch

is not thrown, the door is unlocked, and the switch remains unpressed or uncontacted by the latch.

Here's an image showing the position of the monitoring switch inside a lock:

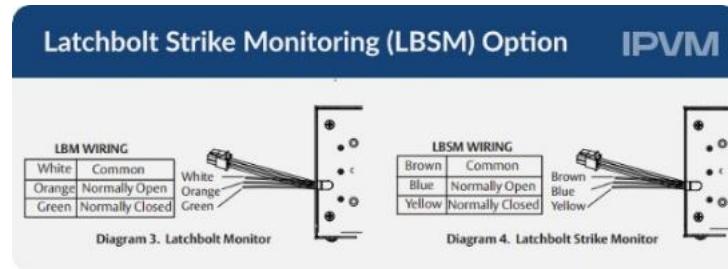


Users should expect approximately this feature adds 5% - 10% per lock, often \$20 or \$30, and adding it usually requires replacing existing locks.

### **Latchbolt Strike Monitoring**

Another method of monitoring strikes involves checking the internal solenoid position, as that indicates whether or no the strike itself is secured for retaining lock latches. The advantage of LBSM is that they are less exposed and less prone to malfunction and breakage, but they are not as common as LBM options on strikes.

Some strikes offer both as an option, like this strike:



## Bond Sensors

The most common method of monitoring maglocks involves a sensor that checks the field strength of the electromagnetic coil inside the unit. When the field is strongest or within spec, an integrated LED or wire output loop signals the lock is firmly bonded. The image below shows the 'green is good' LED indicator on one example:



In many cases, bond sensors are a default option, and using them adds no cost since they are already included. However, these sensors can go 'bad' over time, and the sensitive circuits fail with regular use. Periodic replacement involving a technician onsite and a replacement sensor costing a few dollars may be needed once or twice in the span of five years for these maglocks.

## Using Both DPS and Lock Monitoring Together

For highest security, some installers use both door position and lock monitoring at the same time by wiring the contacts in series with the door position switch. Instead of simply knowing a door is open or closed, the system would see it as open and not secure or closed and secure.

Optionally, lock monitoring outputs may be run to separate general controller inputs. If users want to display door status separately, this method may also be needed to get accurate status. For example, if doors unlocked during the day should be kept closed, separate monitoring from both DPS and lock monitoring is required.

# Advanced Access Openings

## Multipoint Lock

Doors are notoriously weak at stopping entry, and money can be misspent on wrong locks that leave doors quite vulnerable.

While closed and locked doors might deter entry for typical people, breaking in with basic tools often takes mere seconds. In the video below, busting a normal locked door secured by a single lock takes less than a half-minute:

[Click here to view the video on IPVM](#)

However, most doors can be better hardened against these attacks, by installing multipoint locks or latching points. For every latch that is added, burglar and thieves need more time to overcome it, slowing crime so that authorities have more time to react. When multipoint latches are used, simple exploits are made difficult.

We examine multipoint latching, and how it typically is deployed to still be code compliant, yet increase the toughness of doors:

- Door Latches Explained
- Why More Latches Are Better
- What Illegal Latching Looks Like
- The Code Citations Behind Multipoint Latches
- Commercial Multipoint Latch Locks including Detex, Schlage and Securitech
- Passive Hinge Pins Add Multipoint Also
- Configuring Electronic Access To Work With Multipoint Latching

Finally, the 7 question quiz at the end will test your knowledge of multipoint latching.

## Latching Defined

Locking a door usually is a very simple action. "Latching" involves a portion of the door lock or bolt extending or pivoting into the adjacent door frame. Mechanically the operation is simple, and although locks can be quite complex devices, unlatching a door from the adjacent frame is all that is needed to unsecure it for opening. The split image below shows the basic process; twisting the door lever or key turns the latch into or out of the strike plate:



Typical residential and commercial locks work the same way. Often instead of swinging a hook latch, a spring loaded latch pops into a hole in the frame (strikes).

## More Latches are Better

In general, a single latch is easily defeated. Subjected to brute force, the single latching point can absorb little integral damage before it is broken or the frame itself is compromised. Often a kick or hammerblow in the single latch spot is all that is needed.

To overcome this weakness, many doors employ multiple latches. Instead of a single point securing a door into a frame, doors have three, four, or even more latches that protrude on all sides into the frame surrounding an opening.

While defeating these latches may still be possible, it takes more time for brute force to break them all. Given the relative low cost and easy installation of multiple locking latches, it is a common method of improving door security.

### Illegal Solutions Common



Illegal Latches

However, easy and inexpensive it might be, doing it correctly takes careful consideration. Common building codes require that no more than one action unlock/unlatch a door, regardless of how many are securing it.

The most common code citation describing this is NFPA 101:

*7.2.1.5.10 (2009): Where door leaves are required in a means of egress, one of the following criteria shall be met:*

*(b) Unlatching of any leaf shall not require more than one operation.*

As a result, many 'homebrew' and illegal examples of multiple latching can be found, including the door below that includes four additional (extra unlatching operation) pin latches in addition to the door lever lock itself:

For those looking for formal code citations online, see [Free Online NFPA, IBC, and ADA Codes and Standards](#) for area relevant versions and actual code language.

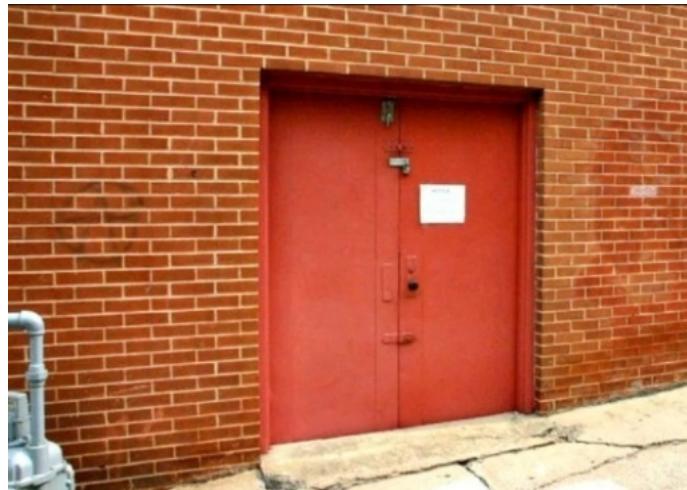
### Common Locations For High Security Doors

Multi-point latching done legally is possible and common. While not an egress door, extreme examples include bank vault doors [link no longer available] that may include 30 or more latching points.

Even in traditional commercial and industrial facilities, these doors are found:

- *Backdoor Retail:* A huge security risk for many retailers is the rear or freight door. The risk of thieves breaking opening this single door and emptying a location of inventory takes mere minutes. Beefing up this door is very common, to mitigate the risk of 'prybar attacks'.
- *Warehouse Doors:* In the same way open backdoors are gateways to valuable inventory, all the doors on the perimeter of a warehouse are a risk.
- *Hazardous/Valuable Item Storage:* Anywhere materials of great value or great risk are stored, multipoint latching is a common sight, even if the area is well within a protected facility surrounded by other access controlled zones.

Especially for non-public, but often still emergency egress openings on the backside of retail and restaurants, finding illegal and potentially harmful secondary latches are common. This restaurant rear door has illegal bolts and latches installed on the outside, greatly hindering emergency egress and violating [basic free egress rules of life safety access control codes](#).

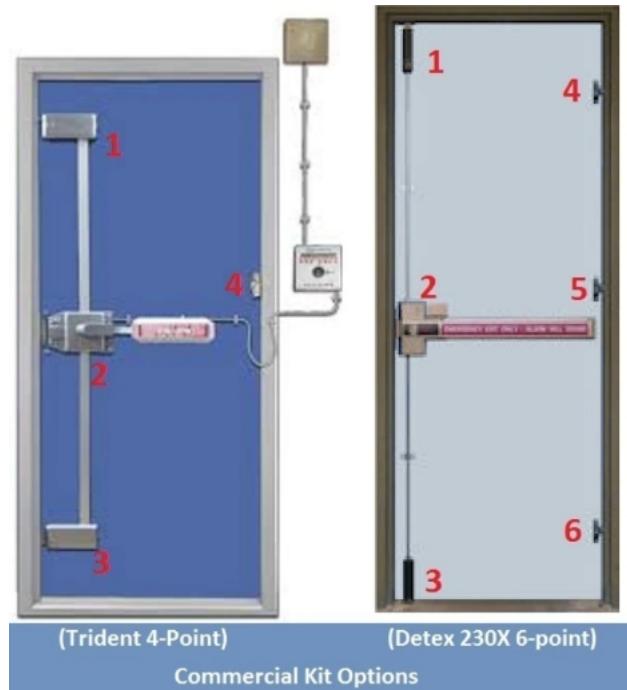


### Commercially Available Options

There are a number of 'off the shelf' mechanical multi-point latching kits available. Usually these kits can be installed in less than four hours, with common hand tools, and by inexperienced installers; although technical assembly and detailed installation skills are needed.

While a singlepoint lockset regularly costs \$300 - \$900, a multipoint lock often costs 2x to 3x more. Some of the more popular units include:

- [Securitech](#): This electromechanical hardware company essentially specializes in multipoint latching but code-compliant door hardware/exit devices. Most kits cost less than \$2,000 but dealer status may be required to buy Trident devices.
- [Schlage](#): Multipoint can be fitted to more than exit devices. Take this [Schlage unit](#) for example, that is a mortise lock with surface mounted vertical rods. This device can be retrofitted to steel or wood doors, and costs about \$1,000.
- [Detex](#): A 'budget' exit device, Detex's 230x costs \$600 - \$1,200 and retrofits most steel doors. [Step by step installation videos](#) are available online, including basic adjustment and troubleshooting.



Usually, commercial kits offer at least three points of latching, and hinge-side pins can be added as needed. For example, the two kits above offer 4 and 6 point latching systems, but the major difference are the addition of more non-mechanical hinge-side door pin bolts in the 6 point kit.

There is no limit or restriction to the number of points used, as long as underlying life safety codes are still satisfied.

As a general rule, the mounting door and frame must be suitable and sturdy enough to support multiple latches. Generally, steel doors and frames with a gauge thickness of 18 or less (thicker) are ideal, but specific kits may require specific door types.

### **Passive Options Improve Security Too**

Not all 'points' in a multipoint system need to be retractable by lever or pushbar. Rather, using the hinge action of a door to separate the leaf from the frame often proves an ideal spot to place security hinge bolts:



The location of the pins means that doors cannot be easily pulled away from the frame. Especially for outward swinging doors, the exposed hinges cannot simply be cut away or hammered open, because the safety pins hold the hinges together unless swung open normally, through the strength of the door locks.

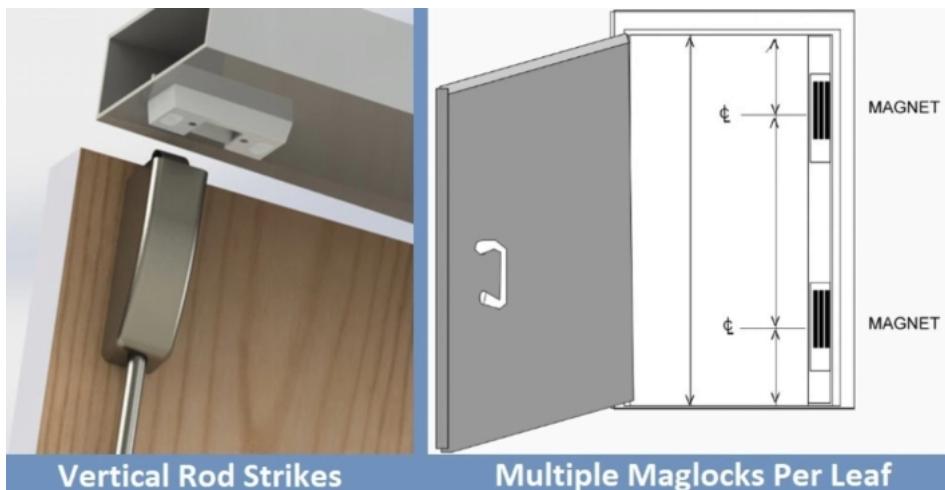
In contrast to 'active' latch locks that may cost thousands, hinge security pins often can be purchased and installed for \$50, and are not impacted by life safety/egress codes because they do not change operation of the door.

### **Access Control Integration**

Generally integrating electronic access control with multipoint latching takes two basic forms:

**Electronic Latch Retraction:** Retrofit multipoint device sets often include a solenoid kit that simultaneously retracts all latching points. However, these kits are generally expensive, costing \$2,000 or more and requiring 5-10 manhours to install and adjust properly. These kits also typically require aggressive adjustment and maintenance or they may not secure the door at all points for proper use.

**Multiple Maglocks or Strikes:** A more difficult to configure method is pairing mechanical latches with multiple electric strikes, or using more than one maglock to secure a door. However, this solution is more difficult to install, because controlling panels need to have multiple outputs for controlling locks, and even then, timing them for synchronized release can be time consuming.



Not all controllers are equipped with multiple lock output relays, and even the ones that do may not permit multiple locks to be synchronized unlocked to support multipoint latching. While most enterprise systems like Lenel, Software House, and S2 support the feature, entry level systems or 'lightweight' commercial controllers and systems like [Dahua Access](#) and [Axis Entry Manager](#) do not.

### Quiz Yourself

Take the [Door Multipoint Latching For Access Control Quiz](#).

# Glass Doors

One of the biggest access challenges are locking and securing glass doors.



Unlike wood or steel doors that can be modified to work with electrified locking hardware, glass doors present great challenges.

We examine:

- Why Glass Doors Are Tough For Access
- Planning Ahead Is Best, If Possible
- The Two Common Types Of Glass Doors
- Glass Door Access Control Options For Readers, Strikes, Maglocks, and Standalone Locks
- Why Using Glues and Adhesives Can Be Trouble

## Glass Doors: Difficult To Modify For Access

Retrofitting electrified locks to 'regular' doors requires drilling or cutting doors, frames, and sometimes both.

For maglocks, the two major pieces of a maglock must be mounted to both door frame and door in order to secure the opening. In most cases, mounting instructions call for drilling a few holes, slipping in a few [sex bolts](#), and nothing more difficult.

However, doors made of glass are a completely different situation. Glass, even thick tempered glass, cannot be drilled or cut once manufactured. Despite being very durable to blunt forces, a sharp hard drill bit, or even a slight warping of the pane can cause a dramatic, expensive shatter.



The solution is not any easier using strikes, because in many cases glass doors are 'architecturally significant' features that are not cluttered up with standard locking hardware. In many situations, standard hardware like hinges, exit devices, and lever sets are replaced with low-profile, custom pieces designed to maximize beauty. The latch bolt a strike depends on to keep a door locked might not even be included!

So, how do you control a door that cannot be modified, may not have rails/frames for mounting locks, and likely uses non-standard hardware anyway?

## **Best Answer: Plan Ahead At The Factory**

The least expensive and 'best looking' electrified solutions for frameless glass doors require the door to be constructed with cutouts, holes, or clearances in mind. Even thin-framed 'storefront' glass frames can come factory prepped for access hardware to mitigate risk against install damage.

Since these changes do not normally add cost and facilitate the best design of the door with locking hardware in mind, planning for electronic access hardware with door manufacturers is the preferred option.

However, electronic access control specifications and specialists are not often included early enough in the design process to impact door design.

As a result, the 'problem' of retrofitting hardware is a common issue. In the sections that follow, we address how to determine which retrofit option is best.

## **Two Types of Glass Openings**

Modern buildings typically use two different types of glass openings. The access control options can vary widely based on which type is used:

### **Thin Framed**

In many retail storefronts and commercial buildings, 'glass doors' are at least partially framed and trimmed by metal sections.



These openings can often use typical access hardware like strikes, maglocks, or latch retraction as long as 'low profile' or 'glass bead kit' versions are used.

### **Frameless Glass**

The other type, more difficult to work with, are 'frameless' or 'butt-jointed' glass openings, also informally called 'Herculite' due to a common brand.

These types have no framing metal, and often no locks or traditional hardware like [hinges](#) or [closers](#):



This style is often used in architecturally significant or minimalist openings and can prove very difficult to find locks that can be installed without factory specification.

Moreover, even if factory prepared to mount locks, networking or cabling the components together can be equally difficult, since there is no raceway or channels to 'hide' conductors inside.

### Retrofit Lock Options

Regular varieties of access control devices are difficult, or not an option, to mount on glass doors.

For these device types we examine options for thin or frameless glass doors:

- Readers
- Strikes
- Maglocks
- Standalone Units

## Readers

In many cases, a thin mullion or wall-mounted reader can be used to control a glass door.

However, when no frame exists, or if a frameless opening is used, readers can be a problem not only due to mounting area but also because of unit wiring that carries power/data back to a door controller.

For these applications, a wireless (battery-powered) reader is an option. Mounting uses adhesive pads and small batteries to hold the unit in place without any cables:



The Securitron R-100, examined in [Wireless Access Control Card Reader](#), is one option. However, battery replacement, limited credential format support, and adhesive becoming unstuck/loose over time can be a big operational problem.

However, in terms of true wireless readers, market options are uncommon, and the Securitron unit uses a Mercury-based interface module that is compatible with many access systems on the market.

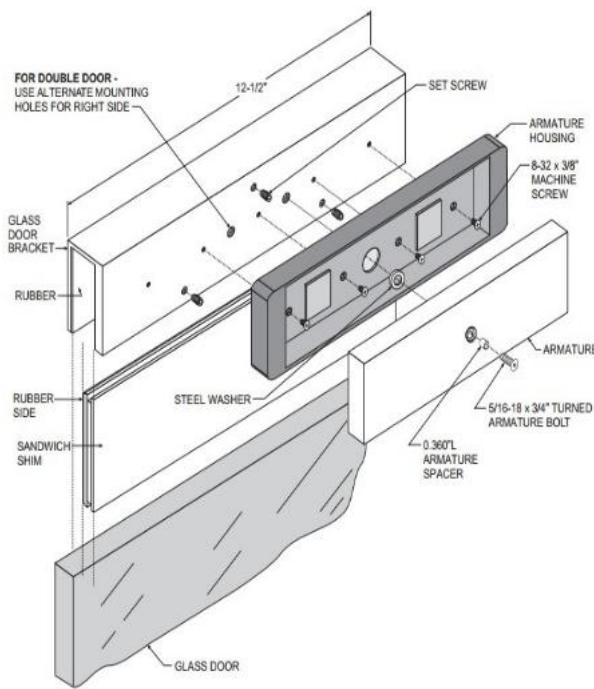
## Strikes

In traditional forms, electric strikes are not generally adaptable to most full glass frameless doors. By design, the strike itself is an integral part of a frame and so one must be present for an electronically releasing version to be fitted.

For this reason, when strikes are used to control glass doors, they are either mounted per specification into a thin adjacent door frame and door lock latch or not at all.

## Maglocks

Retrofitting maglocks to frameless glass doors may be an option, but only when the door uses a top jamb. Several manufacturers [link no longer available] offer a 'saddle' or [sleeve bracket](#) that slides down over the top edge of the door for an armature to mount:

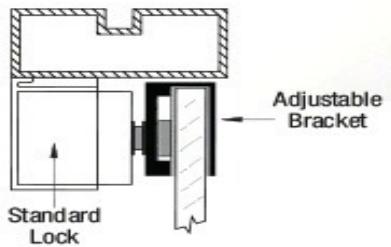


The benefit of this approach is that no drilling or epoxy gluing to the door is required, and the entire assembly is rather strong and secure when the door is shut and maglock is energized. In

most cases, the bracket is held in place with a compression shim adjusted by set screws and is not able to be moved or pried loose.

### Door Header Required

However, while the door/armature installation can be fitted on most glass doors, the assembly often requires the door to be mounted in an opening featuring a top frame to anchor the magnet:



While this arrangement may be available on some glass openings, it typically is not on high volume openings or ones with a significant architectural appearance value, often in main building entries or lobbies.

### Dangerous Floating Top Brackets

Some products may use double compression brackets for doors without headers. However, these products are typically not approved for use because of the dangers they present:



If the top bracket is knocked loose these units might violate code or injure building occupants if they fall from place. Dropping from the installed location may cause the bracket to jam a door closed, or otherwise prevent egress and AHJs should be consulted before use.

## Unnetworked, Standalone Units

Options like [Adams Rite RT1050D](#) is a retrofit keypad, card reader, and mechanical deadbolt that mounts to a door without drilling.

Instead, the unit uses and adhesive-backed mounting clip that secures both the lock and strike plate to the glass door.



The battery-powered standalone lock uses either PINs or MIFARE credentials cards, but is not networkable to existing access control and is strictly offline and standalone.

Another benefit of the RT1050D is that it can be mounted on either single or double frameless glass openings with a maximum thickness of 1/2" or 12.7 mm.

The Adams Rite standalone lock is available from online sources for ~\$350, but is typically discounted when purchased from dealers or in volume.

### Warning: Glue and Adhesive Can Be Trouble

Lacking other options, it is possible to mount 'traditional' maglocks to glass doors using high-strength adhesives and special armature plates. While using standard form factor maglocks for glass may seem the best of both worlds, using mounting adhesives comes with risks:

- *High Skill*: Simply sticking a maglock up on a door may seem easy, but installing it properly with glue takes 'know-how'. Maglock armatures need to be installed so they can move and shift when bonding, and unlike metal or wood, glass doors have no flexibility at all. Unless the installer understands where the armature needs to move, the maglock can break the door.
- *Special Adhesives*: The type of glues or adhesives that can both bond to glass, support the weight of the hardware, and withstand pulling forces equal to the rating of the maglock are very exotic and expensive. Installers may be able to initially mount hardware using [common automotive-type glass adhesive](#), but this bond will fail over time because it is not rated for maglock use. Hardware adhesive kits, like [Securitron's Glass Door Adhesive Kit \(~\\$100 online\)](#) must be used instead.
- *Failed Bond*: Once a bond fails, it results in an immediate security flaw and is very difficult to repair even with new hardware. The adhesives used cannot simply be scraped or sanded off. When a glued bond fails, it often results in replacement of the door and locking hardware.
- *Breakable*: Whether or not glass itself can withstand hammered blows, the brittle bond of glued hardware can sometimes be defeated by knocking it loose. While new adhesives are generally more resistant to jolting blows than old, cold, potentially flaking urethane adhesives, glued hardware is vulnerable to tampering not comparable to physically fastened devices.



# Elevator Access Control

Doors are certainly the first thing that comes to mind when thinking about electronic access control. However, EAC can also be very valuable for controlling elevators. Keeping unauthorized riders out of elevator cars or off certain floors is a significant security benefit. We examine this, breaking down the two main methods of control, how to integrate access control for each, plus how to deal with the key risk of tailgating.

## Two Methods

Securing control of an elevator system has two options depending upon the desired level of control. Determining which method is best depends on which of the following two is more important:

- *Unauthorized access to specific floors, or*
- *Unauthorized use of the elevator?*

For example, if keeping people from 'nuisance calling' the elevator or to prohibit anyone except credentialed personnel from using the lift, controlling the call buttons is often the best solution. However, if administrating access to specific floors is required, then the car must be equipped with a controller that interfaces access levels with the elevator's mechanical systems.

The two methods vary broadly in cost of equipment and integration; points we examine in the following sections:

*Interrupt the Call Buttons:* Of the two options, this level of integration is simpler and inexpensive, but only provides "all floors, or nothing" control. This involves wiring the power of the call button keypad to be switched on according to credential reads of an adjacent reader. In order to activate the call buttons to request a car, the controller closes relay contacts between

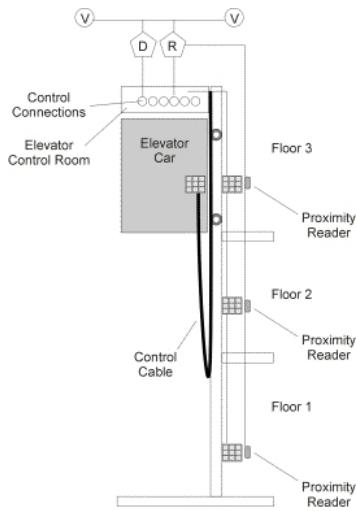
the call button's power supply and keypad. Only a card granted access to the elevator is eligible to use the elevator, but once the elevator arrives, the user is able to key access to any floor the elevator normally has access to; potentially all floors in a building.



The biggest advantage afforded by this method is how inexpensive and quickly it can be installed. The process of integrating call button power to a controller often requires an [external relay](#) of some type, but otherwise it schematically installs and performs like access through any other opening, except with outputs routing power to buttons rather than door locks.

The second method is more challenging.

*Controller Onboard:* This method requires deeper integration, specialized equipment, and higher configuration costs, but results in a greater degree of control to specific floors rather than the car itself. Take this manufacturer's example schematic below:



With this type of integration, the position of the car relative to a floor is fed back into the controller, typically installed on the cab itself, or connected to the cab via the travelling 'control cable' networking the car to its mechanical control system. Users are configured access to specific floors; for example, a rider may be able to call an elevator from 'Floor 1' and only be able to ascend to 'Floor 3' based on access rights, bypassing 'Floor 2' altogether.

This method requires interfacing the access control system with the elevator control system, and may require coordination with the elevator company's service technicians.

*Traveling Cable:* Another complicating feature of onboard control is networking components like readers and controllers to the 'head end'. Mounting the controller onboard the car is not often required, but is done to mitigate the need of running expensive, maintenance hungry elevator cables to connect components. As we noted in our "[Elevator Surveillance Tutorial](#)", networking devices in a moving car is prone to a host of cabling issues complicated by the notorious difficulty in coordinating work with Elevator Service Technicians.

### Tailgating Risk

Regardless of the method chosen, access control is endangered by '[tailgating](#)', that is, an unauthorized person passing through a controlled opening before it is closed and relocked after a valid credential read. In the case of either elevator control options above, an unauthorized

person can both enter a car before the doors close, or exit into a restricted floor when someone else leaves.

Elevator safety interlock controls [link no longer available] always incorporate some manner of keeping doors from automatically closing and potentially crushing or moving before occupants are completely onboard. One characteristic of these controls are the slow closing speed of the opening, a variable that cannot be addressed by the EAC system. Because of the life/safety risk, ensuring access control can only be achieved via limiting occupants in a car to a single passenger or expanding access controls to doors beyond the elevators.

Because of the tailgating risk, some end-users question the security value of access controlling elevators. Rather, the strongest benefit of controlling elevators comes in the form of restricting use, leading to increased car availability for VIPs and lowering the occurrence of vagrancy inside elevator cabs.

## Turnstiles

Turnstiles control pedestrian access to secured areas, essentially becoming moving portions of fences, walls, or barricades for physically stopping intruders.



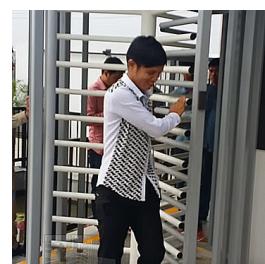
However, they can be ugly, expensive, ineffective, and downright dangerous if used unwisely. Inside we examine the common types of pedestrian turnstiles and examined the strengths vs weaknesses of each type:

- Full Height
- Half-Height
- Optical
- Turnbuckles
- Revolving Doors

We demonstrate how to calculate the number of turnstiles needed as well as prepping, installing, and maintaining them.

### Turnstile Function

When it comes to access control, few engineering controls can be as effective as turnstiles.



They typically have a physical barricade or barrier that pivots freely when access is authorized, allowing only one user entry at a time:

From a security standpoint, turnstiles are used to:

- Restrict Access To/From An Area
- Count People Flowing Through Areas
- Checkpoint Traffic Restriction

[Click here to view the animated gif on IPVM](#)

The design of these spinning gate sections can essentially mitigate [Tailgating](#) risks and otherwise force every user entering a controlled area to register with the access system.

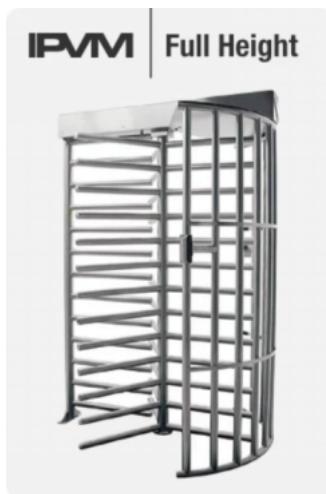
## Turnstile Types

In the sections below, we examine the common types of pedestrian turnstiles and examined the strengths vs weaknesses of each type:

- Full Height
- Half-Height
- Optical
- Turnbuckles
- Revolving Doors

### Full Height

These turnstiles are revolving gates that extend to a height of 7 to 10 feet. Typically, they are designed to be adjoined on both sides by fence or wall.



These are the most secure turnstile type, due to the difficulty in passing around or over these units when secured, but they are also the most unaesthetic, take up significant space, and are costly. In general, [Free Egress](#) can be maintained by allowing them to be 'free-spinning' in egress directions, but the actual models and sizes of turnstile must be reconciled against [Life/Safety Codes](#).



These types of turnstiles are best used when monitored entry through perimeter security is required at fences or main entries. These turnstiles cost about \$5,000 USD for a single sized unit, ~\$10,000 USD for a double-sized unit, and often can take multiple days and multiple laborers to install.

## **Half-Height**

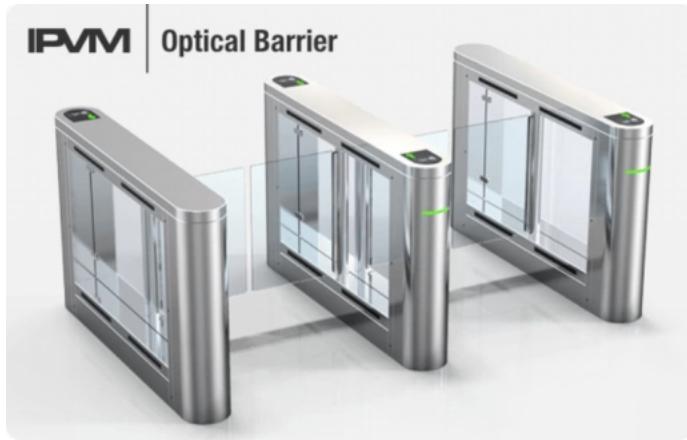
This type of turnstile is used to restrict free access to specific areas, but are not as physically imposing or large as full height units:



These units are valuable pieces of choke-point design for controlling speed and position of pedestrian traffic. They are often mounted in groups of two or more. These units are easily jumped over and are not appropriate for high-security applications. These units are best used to regulate foot traffic flow into other areas. These turnstiles cost about \$4,000 USD each.

## **Optical Turnstiles**

This type is a variation on the waist height turnstile with a lightweight physical barrier arm, and is implemented for 'administrative access control' rather than physical control:



The primary feature is to monitor/count traffic by use of wireless beams, [Time of Flight](#) cameras, or [pressure pads](#). These units are typically heavily integrated with access control systems to detect tailgating into an area. These turnstiles use sirens, lights, and perspex or plexiglass barricades for access control:



[Click here to view the animated gif on IPVM](#)

Units often have cutouts or integrated credential readers onboard. Optical barrier turnstiles are best used to monitor public access for large buildings like areas or convention centers. Pricing varies with options, but a typically equipped optical turnstile start about \$5,000 USD, but can range significantly higher to ~\$30,000 USD per lane.

### Turnbuckles

The weakest turnstile type is also one of the most common, often used to check paid admittance into an area rather than strict physical access control:



The basic construction of a turnbuckle are pipe or tubular sections that rotate around a spindle, and the physical barrier is often mostly forced standoff distance between people entering the area.



Pricing for turnbuckles generally starts at ~\$500 USD for single units, although multiple units are typically installed together.

### **Half-Height & Turnbuckle Vulnerability**

The primary risk with less than full height turnstiles is that intruders can just jump or climb over them, as is [common with 'fare-jumpers'](#) in mass transit systems:



For this reason, these turnstiles are often combined with other systems like cameras or manned security staff to monitor the areas where they are deployed.

### Revolving Doors

One of the most aesthetically pleasing, yet expensive turnstile types are revolving doors. This turnstile type is often sold as a [Mantrap](#). The function of these doors is the same as Full Height turnstiles, but the chambers are frequently sized for occupancy fitting more than a single person:



While access control potential is strong, costs and installation complexity are also high. Simple single-door kits can cost \$8,000 USD and main entry high occupancy retrofits can cost ~\$25,000 USD or more and require substantial architect and trade labor involvement to install.



### Mandatory Gates

One of the most common problems with turnstiles is accommodating those who cannot use them but still need access.



Often, regulations dictate the inclusion of [ADA/Pedestrian Gates](#). These are gates that permit wheelchairs or carts through a secured, swinging opening as an alternative to the inaccessible turnstile. Gates are often located adjacent to turnstiles and are included in the same access

administration point. When used with access controls, specific individuals can be credentialed to travel through gate rather than turnstile.

Gates may also permit an entry point for supply carts to travel through a fence line rather than the spindled turnstile. Including at least one of these gates in a fence-line is common, and it is prudent to locate them adjacent to handicap parking areas or load/unload areas.

### **Proper Sizing & Unit Counts Needed**

Sizing is the most important factor when planning turnstile placement. These considerations significantly affect the total number of turnstiles required to do the job. If the number of required turnstiles seems unrealistically high, consider staggering shift changes to permit more time for traffic to flow.

The number of turnstiles must be 'sized' according to the traffic volumes they must handle. This sizing is a rough calculation for how many people can travel through the turnstiles in a given period of time:

### **Sizing Example**

Consider the following design example:

You have been asked to furnish a quote for the number of turnstiles at the front employee entrance to a manufacturing plant. Full height turnstiles will be installed at the main fence line separating the parking lot from the plant building.

There are 2,000 employees arriving for work during this change, and 15 minutes have been set aside for this exchange of workers. How many turnstiles should be quoted for this job?

Answer: The resulting calculation determines that 17 - 18 turnstiles are required to handle 2,000 people in 15 minutes. A typical full-height turnstile is designed to accommodate 450 - 500 per hour. The average pass-through rate is 8 people per turnstile, per minute. If 2,000 people

must flow through turnstiles during a shift change, consider the time to handle that volume is limited to 15 minutes.

$$\text{(Total Number of People) / ((Flow through turnstile per min) * (Number of mins available))} = \text{(Number of Turnstiles)}$$
$$(2,000 \text{ people}) / ((8 \text{ people per minute}) * (15 \text{ minutes})) = (16.7 \text{ turnstiles})$$

Since turnstiles are furnished in 'single' or 'double' sized units, furnishing a quote for 18 turnstiles (or 9 doubles) is prudent with a slight over-sizing of the number of turnstiles for the occasion that a unit is out of service.

### **Site Prep**

Installing turnstiles often require concrete pad preparation and fence cuts. This work should be carefully planned and communicated, as a gap in fencing may be present for an extended period of time. Security should be notified of these gaps, and extra supervision or policing of the area may be required until turnstiles are installed. Dirt work or setting concrete forms may be required and routing electrical and data utility is typically needed as well.

Area lighting and cover from the weather may be needed, especially when mounting turnstiles outside. Other security systems like surveillance and intercoms are often installed at these points to assist turnstiles for access control.

Turnstiles are not typically low-voltage machines and installation work often must be coordinated with an electrician. This can be an especially tricky part of the job considering that turnstiles are often located in the elements and on distant fence-lines.

The additional site prep elements can double the cost of implementing the turnstile alone.

## Integrating With Access Control

In most cases, turnstiles of all types can be integrated with access control, often using the same system settings and logic as doors.

Instead of a hinged door lock or strike, the turnstile spindle or solenoid is connected to an [Access Control Door Controller](#) and users scan credentials using traditional [Access Control Readers](#) mounted on bollards or mounting plates on the turnstile itself:



Most commercial turnstiles have factory options to integrate with access control, and even basic systems can typically integrate them.

## Installation

Where possible, turnstile equipment should be 'drop shipped' directly to the installation site. Depending on the type and number of turnstiles to be installed, the equipment weight may be several thousand pounds.



Due to bulk and weight, a [material lift](#) may be required to move and install this equipment. Installation of most turnstiles should be considered a 'two-man' job, due to the unwieldy bulk of these units, but most units can be installed in two typical workdays or less.

## Maintenance

Turnstiles are often located outside in harsh weather and are heavily used at critical security points. As a result, some periodic maintenance should be planned to service these machines.

Weatherproofing electronic equipment and keeping mechanical parts lubricated and adjusted should be considered an ongoing part of operating these units. In many cases, the turnstile manufacturer will offer a semi-annual 'maintenance kit' of replaceable rings, seal, and grease, and the installer can offer this in a Service / Maintenance Contract.

[Note: This guide was originally written in 2012 but substantially revised in 2019.]

## Mantraps

One of access's primary goals is keeping people out of places they should not be, but slipping through open doors (ie: [Tailgating](#)) is often easy.



For high security locations, strict access controls often require the physical opening itself to help restrict access, and mantraps are one of the most effective methods of doing this.

We examine these key six mantrap factors:

- Using Mantraps vs. Turnstiles
- Mantraps have been used for hundreds of years
- Revolving doors can be used as mantraps too
- Mantrap cost
- Vehicle mantraps called 'Sallyports'
- Free egress still applies

### Using Mantraps vs. Turnstiles

For some applications, the choice between mantraps or turnstiles (see our [Turnstiles Guide](#) for more) appears largely aesthetic, but mantraps are 'higher security' than turnstiles alone.

With mantraps, several security risks with turnstiles like jumping over them, throwing objects into protected areas, and potentially allowing intruders to escape are mitigated:

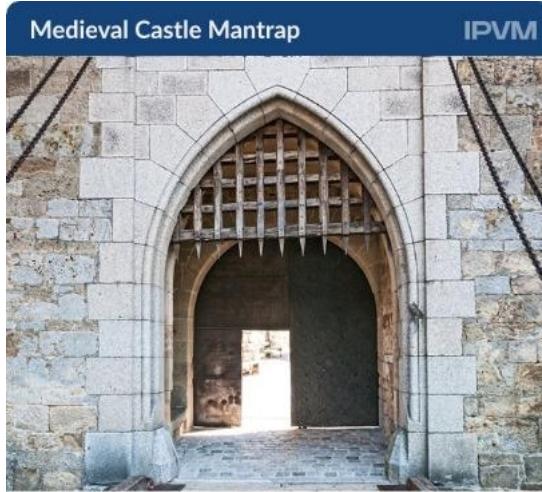


In many cases, turnstiles look 'institutional' and harsh while mantraps offer more access control, they also can often be constructed in an architecturally pleasing way:



### Mantraps Used for Centuries

One of the oldest techniques in access control is still used today. Mantraps date back to medieval times for mandating access is only granted to specific people, with the added benefit of 'trapping' an intruder.



Modern uses of mantraps vary and have expanded over the years, but the concept is still applied in many facilities today.

### **Mantrap Theory of Operation**

The clip below provides a simple example a mantrap in use:

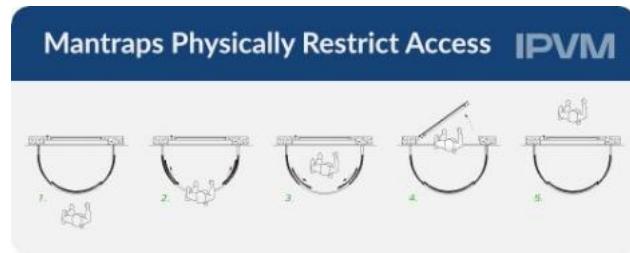
[Click here to see the mantrap tailgating video on IPVM](#)

Notice the key attributes of how it works:

- The outside door freely opens without any lock, until the inside reader scans a credential
- The inside door unlocks, and the outside door locks, preventing anyone from entering the 'passthru' room.
- The outside door remains locked until the inside door closes and relocks.

The 'interlocked' nature of the passage allows only one door to be unlocked and open at a time. Aside from restricting access, the benefit of the interlock can permit the environment inside the room to be normalized (temperature, pressure, dust) before introducing it to the inside area, or even disinfected. When used this way, "mantraps" are often called "airlocks", but even when security is not the primary goal, the logical sequencing of doors is the same.

The schematic below shows the path one would take, first entering through the curved door, waiting for it to close, validating access and then opening the next interior door.



## Revolving Doors

One of the most aesthetically pleasing, yet expensive turnstile types are revolving doors. This turnstile type is often sold as a mantrap. The function of these doors are the same as Full Height turnstiles, but the chambers are frequently sized for occupancy fitting more than a single person:



While access control potential is strong, costs and installation complexity are also high. Simple single-door kits can cost \$8,000 USD and main entry high occupancy retrofits can cost ~\$25,000 USD or more and require substantial architect and trade labor involvement to install.



### **Mantrap Cost**

On a cost basis, coordinating sets of doors via controllers via interlock configuration is generally the least expensive option if access is already being used.

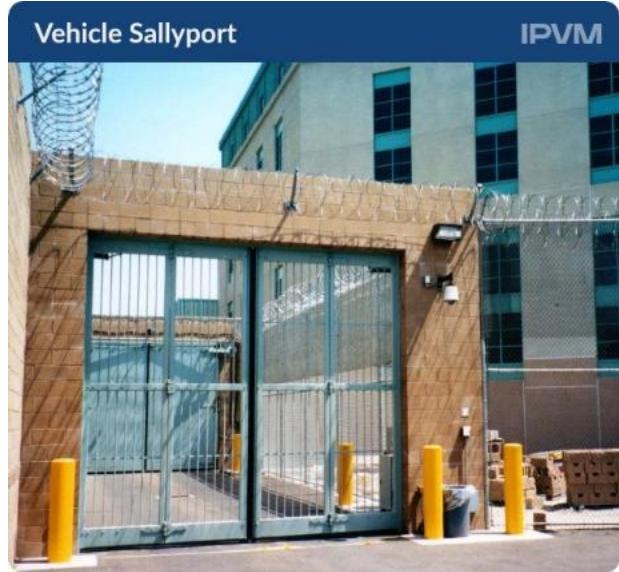
Retrofit ['kit' or booth mantraps](#) typically cost ~\$7,500 - \$10,000, but this price may be less expensive, less disruptive, and quicker installing than custom ['stick built'](#) mantrap.

For revolving doors, single-door kits can cost \$8,000 USD and main entry high occupancy retrofits can cost ~\$25,000 USD or more. These options often require substantial architect and trade labor involvement to install.

### **Vehicle Mantraps: Sallyports**

Aside from regulating pedestrian ingress into a space, mantraps are also employed to prevent vehicle intrusion in security-sensitive access controls like 'Sallyports'.

Many jails and most prisons include this feature, so that a suspect or prisoner can be unloaded from a police vehicle without having opportunity to escape.



In many cases, a sallyport interlocks the function of a jail/prison door with a garage-type overhead door. In cases where the overhead door is up, the jail door is locked, preventing inmates from escaping into the outside grounds.

Likewise, when the overhead door is down, the inside door is unlocked, allowing a suspect the enter the booking/holding area, but unable to escape to the outside grounds.

### Safety Codes still Apply

The relevant codes that apply to use of maglocks depend largely on the [occupancy code classification](#) of the facility. For example, a penal institution or jail is classified differently than an office building and is exempt from many of the 'life/safety' protections required. Checking to see which codes apply first requires a clear classification of the building type.

For most commercial/education/industrial classifications, Life Safety remains the 'golden rule', which means that free egress must always be maintained. In this case, mantraps can be used to keep people out of an area, but they cannot be used to hold people within one.

## Free Egress Often Required

IPVM



In many cases, standard RTE override hardware and fire alarm interfaces are required, so that in an emergency no one can potentially be trapped inside a "passthru" room.

## Vehicle Gate

Vehicle gate access control demands integrating various systems to keep unauthorized cars out.



Everything from high voltage electrical, to concrete modification, trenching, welding, low voltage systems (<50 volts), and manual labor is required to accomplish a fundamental task of access: keeping the bad guys on the outside of the fence.

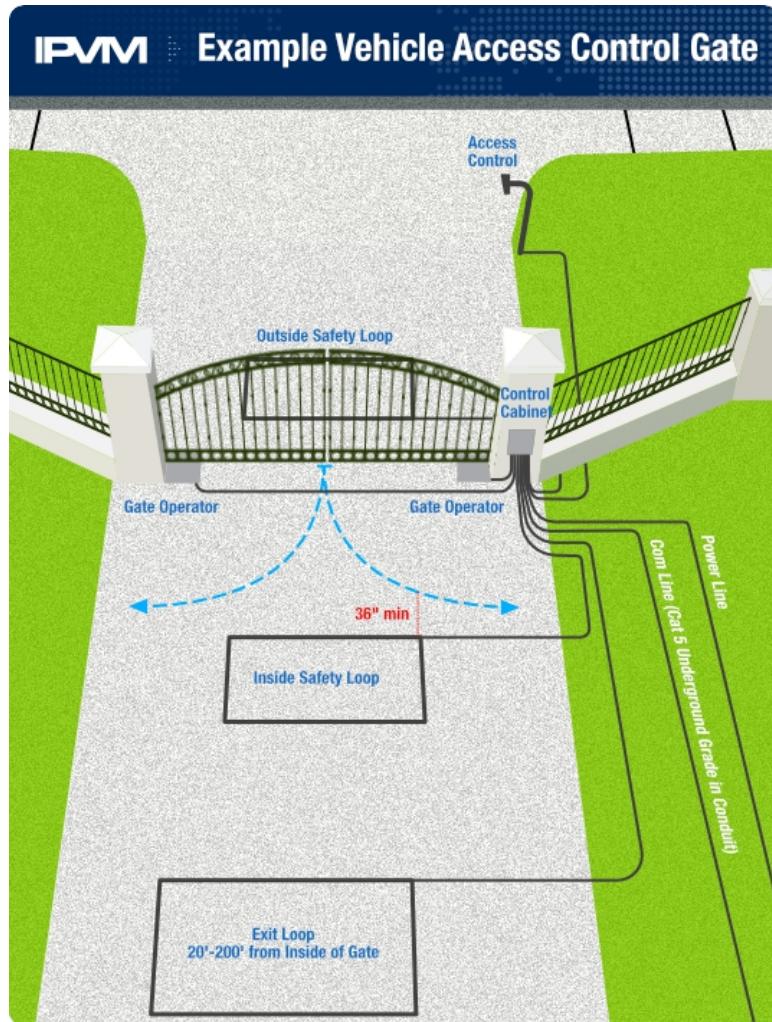
We examine the various facets of gate access, from design to install, and even the special equipment needed to get the job done.

- Defining what 'Ground Loops' Are
- Answering Why Vehicle Gates Require Them
- Special Card Reader Pedestals
- When Long Range Readers Are Needed
- Integrating High Powered Operators
- Why Intercoms and Lights Are Important

## Gate Access Design

The most common method of restricting vehicle and pedestrian access at property lines is through fences and gates. While security integrators are not typically tasked with designing or installing perimeter fences, many find themselves working to integrate access control with them.

The image below is a typical example of how a gate is integrated with various systems to work with electronic access:



The major parts of the system are typically only used with vehicle access applications:

- Inductive Ground Loops
- Long Range Readers
- Reader Stand/Bollard Design
- Gate Operators
- Integrating EAC to Operators

General tasks like trenching are still vital skills to leverage properly on the typical gate job. See our [Cable Trenching for Surveillance Guide](#).

## **UL325 & ASTM F2200 Specifications**

In terms of design standards, [UL 325](#) & [ASTM F2200](#) often are required by code.

While mostly relating to product design requirements, they define how a spec conformant product should be installed so the safety features work properly.

In general, those mandate the inclusion of photo-beam devices and roller/chain covers to protect against crushing/pinching.

The specifications vary based on the type of gate installed, ie: Swing/ Slide/ Vertical Arm, but generally describe how highly PE beam detectors should be installed, rolling clearances, and how the gate 'fabric' itself should be fitted to avoid catching people into the action of gates.

### **Inductive Ground Loops**

Specialty sensors called 'Ground loops' are used to sense vehicles by the gate operator. The use of ground loops is widespread, as most traffic signals or intersection lights use them to detect vehicles.

Ground loops emit an inductive field at a constant state. When a large metal object (like a vehicle) enters the field, the constant inductance of the field changes, signalling the presence of a vehicle and triggering devices like gates to open or close.

Induction is an electromagnetic measurement, so a non-ferrous mass like a human or animal does not influence the field. Typically most ground loops are tuned so that even small metallic masses, like bicycles, carts, or barrels will not 'trip the sensor', and they only will respond to vehicle traffic.

For gate access projects, a number of ground loops are used:

- Exit Loop: This loop is installed a distance away from the gate, primarily so that the gate is fully open before the moving vehicle reaches the gate.
- Inside Safety Loop: Essentially this loop is used to detect the presence of a vehicle in the path of a swinging gate. While the necessity of this loop depends on the type of gate being used, most recommend a stand-off distance for clearance of the moving section.
- Outside Safety Loop: In many cases, this loop is used as a form of 'anti-tailgating', where multiple vehicles can 'stack' behind a closed gate and pass through based on a single credential read. Again, the requirement to use this loop changes based on gate operation, but many employ it to ensure only the vehicle that credential passes through.

Installing ground loops are simple, but likely unfamiliar for many installers. Inductive loops are typically lengths of cable. The size and location of the loop vary according to the manufacturer, but installing them involves cutting small grooves (kerfs) into concrete, threading the loop into the channel, and then sealing the top with a non-ferrous, resilient polyurethane or tar. Even when installing loops into 'new' concrete, the cutting process is used, rather than embedding, because the depth of the loop into the concrete must be tightly controlled.

The image below shows this process, notice the installer is 'seating' the loop at a pre-cut depth into saw grooves:



Sawing concrete requires a high powered saw with special blades. The operation of the saw is like other circular saws, where the depth of the cut is determined by guides. The actual cutting action may be 'wet', where water is run over the blade for cooling and to lubricate the cut.

Most construction equipment rental companies, and even home improvement retailers offer concrete saws for rent. The amount of saw cuts for a typical gate job is modest, and most can be done with a handheld tool:



### Reader Mounting

One area where 'thinking outside the box' pays off is reader mounting design. Because various vehicles pass through gates, multiple readers or other system stations may be needed at gate entrances.

Considering occupant ride height differs greatly between the average sedan and diesel tractor trailer, the best solution is often to create a 'dual mount' with a low station and high station.

The image below is an example of a 'right driver' sided vehicle, for 'left driver' countries this arrangement is typically mirrored:



Notice other details about this particular install: protective bollards have been installed adjacent to the reader station to prevent damage if a vehicle strikes the stand. Bollards are sturdy, permanent barriers to ensure a stand-off area between equipment and vehicles.

### Long Range Readers

While not exclusive to vehicle gates, long range readers are most typical of this application. Unlike mullion mount readers that measure a few inches tall, the internal antenna and power

requirements of a long range proximity style reader can grow large, even to ~24" square or larger.

The use of these readers typically allows a vehicle to permanently mount a sticker or token to the windshield glass, have it read at the gate, and leave it on the vehicle. Because 'long range' may still mean less than 15' for many credentials, the vehicle must stop relatively close to the gate and wait while it opens:



If a 'rolling entry', or passing through the gate without stopping, is required a longer-range reader/credential technology is often needed. Typically microwave or UHF band RFID readers are used for this purpose, but this may require an additional credential type specific to the reader to be issued and maintained.

For more, see our [Long Range Access Control Readers Tutorial](#).

### Gate Operator Interface

One of the most critical and potential complex aspects of vehicle gate access can be simplified by keeping one thought in mind: The gate should be integrated just like a door. However, rather than controlling a strike or maglock, the access system must trigger the gate's 'operator', or movement mechanism.

Opening a gate and interfacing with all of the potential sensors and outputs is a complex task. The gate itself may need to be specially timed or sequenced to open safely and reliably. While many door controllers have the inputs, outputs, and configurations needed to control the gate opening, it is best to use the operator for that purpose, and only integrate the EAC controller to trigger the gate to open or close based on credential reads.

Gate Operators vary widely according to the exact style of gate they are matched with. The physical size, weight, speed, and opening action of the gate are all factors in selecting the right operator. The type of gate is typically matched to the application and falls outside of this note. (For a comprehensive look at the different styles of security gates available, see our '[Security Gates Tutorial](#)'.)



However, regardless of the type of operator used, the method of interfacing the access control system and the gate is the same: input contacts. The image below is a general example of an operator control board, with the EAC inputs called out:



Standard door controllers or reader interfaces are wired directly to the inputs of the specialized gate operator, and all the nuances of open, closing, and sensor inputs take place in the operator itself.

### **Intercoms and Lights Are Important**

Because vehicle gates are typically long distances from buildings, getting help to users who have lost their credentials, or handling visitors can be a real challenge.

For this reason, best practices use intercoms at reader stands so the possibility to lend assistance is easy and discourages the potential of propping gates open similar to the risks [Propped Doors](#).

The inclusion of intercoms, or even video intercom stations at the gate keeps unauthorized people outside, yet allows them to solicit help if needed:

## Intercom Stations Useful At Gates

IPVM



Another 'smart' accessory is hanging status lights at the gate or even on the barrier arm:

## Barrier Arm Notifications & Signals

IPVM



Given the operation of the gate and position of the barrier may be confusing to unfamiliar or distracted drivers, installing a highly visible and simple light stand or signal is prudent. Using basic colors for driver feedback (ie: red means 'stop', green means 'go', yellow means 'error'), an access system can communicate with drivers using the typical connection used by LED connections for readers.

# Credentials & Readers

# HID vs NXP Credentials

Two companies dominate the global market for access control credentials: HID Global and NXP Semiconductor. Both companies own or influence huge chunks of the credentials game, so which one should you choose? We explain how their offerings differ, interoperate, and how the choice impacts system selection.

## Credentials Dominated by Giants

Upwards of three quarters of the credentials market uses formats developed or licensed by [HID Global](#) and [NXP Semiconductor](#).

### *HID Overview*

Since the market began migrating away from 'magstripe' credentials in the mid 2000's, [HID Global](#) rose to prominence with its 125 kHz "Prox" offerings. After being purchased by ASSA ABLOY, the company became 'the credentials house' for a huge swath of the security market, and OEMs products for access brands like Lenel, Honeywell, and Siemens. The company's best-known formats include:

- "Proximity [link no longer available)": an older 125 kHz format, but still regularly used and specified even in new systems
- [iClass](#): an HID Global specific 13.56 MHz 'smartcard'

HID is the 'defacto' choice for credentials in the US. Because of commanding market share, HID is able to license the use of its credential formats to a variety of credential and reader manufacturers. Even when marketing general 'ISO 14443 compliant' offerings, HID strictly follows "Part B" standards (vs Part "A" - described in more detail later).

## *NXP Overview*

Formerly Phillips Semiconductor, [Europe-based NXP](#) offers a number of 'contactless' credential components used in a number of markets - security, finance, and industrial. With widespread adoption of ISO standards in credential specification, NXP offers a catalog of types built to spec, including:

- [MIFARE PROX](#): NXP's 125 kHz format built on early drafts of ISO standards, but not as widely adopted as HID's "Proximity" lines
- [MIFARE/DESFire](#): an ISO Standards based NXP 'smartcard' format, also operating on 13.56 MHz. The 'DESFire' moniker was introduced in the early 2000s to distinguish the format from 'MIFARE Classic' credentials. DESFire credentials feature stronger encryption that required higher performing chips. The 'Classic' format fell under scrutiny for being [vulnerable to snoop attacks](#), and DESFire countered this threat. Because these improvements were made only to credentials, and existing MIFARE readers could still be used, the new format became known as 'MIFARE/DESFire'.

Unlike HID, NXP's credential formats are 'license-free' and the according standards are available for production use for no cost. NXP manufacturers all ISO 14443 product to "Part A" standards.

## *Other Credentials*

To a much smaller degree, other RFID-based data formats sporadically pop up in physical access control, including:

- [Gemalto IDprime.NET](#): IT-centric smart card format, originally used for logical access credentialing built on .NET framework
- [Sony FeliCa](#): Widespread use in Japan, especially for cashless proximity systems (mass transit, banking)

While not widely used in access control, those formats accomplish the same primary task and use the same basic methods of doing so as the 'market giants'.

## US vs the World

Because of NXP Semiconductors's strength in [EMEA](#) and the lack of licensing, MIFARE, DESFire, and the associated derivatives are popular pretty much everywhere outside the US.

However, HID Global's strongest markets are in the Americas, especially in the US. Despite the additional cost of licensing compliant credentials and readers, [the company also produces product that uses the unlicensed NXP formats](#) and has equal or greater operability as a result.

## The ISO/IEC 14443 Division

Very little separates HID's iClass from NXP's MIFARE offerings, and if not for ambiguous interpretation of an ISO standard, they would 'look' the same to most readers. However, because early versions of the standard left room for differentiation, HID and NXP designed their 'compliant' standards with a different encryption structure.

The end result of this is both versions of credential claim '[ISO 14443 Compliance](#)', but are not entirely interchangeable. To reconcile this difference, ISO revised 14443 to include parts 'A and/or B' to segregate the two offerings. Some aspects of these cards are readable across 'Parts', but any encoded data is unreadable between the two.

In general, because there is no licensing cost in using 'Part A' standards, many low-cost and new products start here.



Meanwhile, readers marketed specifically in the US or from vendors with a broader global market license use of 'Part B' compliance from HID:



## Both ISO 14443A & B Adoption

However, determining which 'parts' a reader or credential is compliant with is not always listed, and confirming a specific brand/type of credential can be used is required.

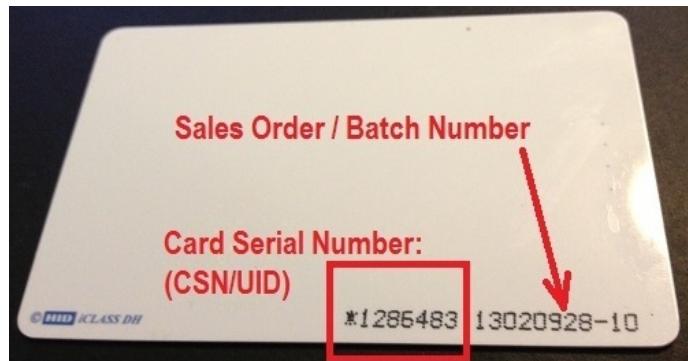
### Interoperability

While the 'Part A & B' division in ISO 14443 separates formats from being the same, it does not always mean they are unusable with each other. Portions of ISO 14443 are the same in both parts, including the 'Card Serial Number'. For some access systems, this is the unique number that identifies unique users, and because this number is not encoded, it will register in 'non standard' readers:

- *CSN/UID String:* Essentially the card's unique identifier is readable because it is not stored in the deep 'encrypted' media. Many simple EAC platforms use only this number

to define a user, and instead use the internal database to assign rights, schedules, and privileges.

- *Encoded Read/Write:* However, the vast majority of storage within the card is encrypted and unreadable unless compliant readers are used. Especially for access systems using the credential itself for storage (eg: Salto, Hotel Systems) and for multi-factor authentication (eg: biometrics) high security deployments, the simple CSN is not sufficient.



### System Impact

In terms of access systems, credential providers/formats matter most during design. Reader selection must consider the credential format, and all subsequent badges or fobs must agree with that choice. In terms of 'Access Management Platform' selection, this format does not generally matter, because the reader itself negotiates credential communication. As long as the platform is compatible with the reader, credential choice is a marginal impact, and most specify credential types based on logistics and ease of purchase rather than technology difference.

However, once this decision is made, changes are costly because they typically require replacement of credentials or reader devices. Changing from one format to the other can cost thousands and affects all users, so changes are uncommon.

## Access Credential Form Factor

Deciding which access control credential to use and distribute, including form factor, can be a difficult task.



Knowing the limitations and strengths of common form factors will help the integrator recommend the right choice.

We examine the most common form factors available, describe the design attributes of each, and describe where they best are applied. The common 'form factors' of credential are:

- Card/Badges
- Clamshells
- Key Fobs
- Stickers or Tokens
- Embedded Chips
- Mobile Credentials

### Common Credential Form Factors

While the components of access credentials are small enough to fit into many different shapes, like [embeddable capsules](#) or [jewelry](#), the most common forms used in access control are:



## Card/Badges

This format is the popular thin, flexible plastic card that many people associate with electronic access control.

The physical size of this credential varies. The most common size of this credential is described by [ISO 7810 ID-1](#) or 'CR80', but other sizes exist. The variation in sizing is considered to be a security attribute by some because unique sizing makes the credential difficult to counterfeit.



Because the user can directly print images on these cards, they commonly double as Picture ID badges. Badges often can be printed or purchased to contain a number of unique ID elements including:



These are inexpensive credentials, designed to be inexpensively replaced. Sometimes these credentials are even considered 'disposable', like hotel keycards or public transit passes. Blank card credentials can be purchased from distribution for about \$0.70 to \$7.00 per piece depending on [which format is needed.](#)

### Clamshells



In contrast to the 'card/badge' format, clamshells are thick, rigid pieces of plastic. This bulky form factor withstands abuse better than cards and may be cheaper than other more durable options.

Clamshell formats are often older than 'card/badge' credentials, and they were designed to accommodate larger (older technology) components. These credentials can be made into picture IDs by applying a preprinted label.

The cost of this form factor depends heavily on the other design characteristics of the card. Clamshell credentials can be purchased from distribution for about \$0.50 - \$8.50 per piece.

## Key Fobs

Fobs are small devices intended to be located on keyrings.

While these formats are not printable, they are very durable and can withstand harsh punishment. These credentials are designed to be crammed into pockets, dangle roughly from keyrings, and endure exposure to all-weather environments.



This form factor is expensive compared to other options, however, they are designed to be replaced much less often. These credentials can be purchased from distribution for about \$1 - \$8 per piece.

## Stickers or Tokens

This form factor is often applied to other items (like the heads of keys). This format is useful for making other devices 'hybrid' credentials.

This format's primary advantage is that they can quickly be externally applied to other devices. For example, applying this type of sticker to a car windshield is a common method of credentialing through vehicle gates.



Other forms include windshield stickers or 'dogbones':

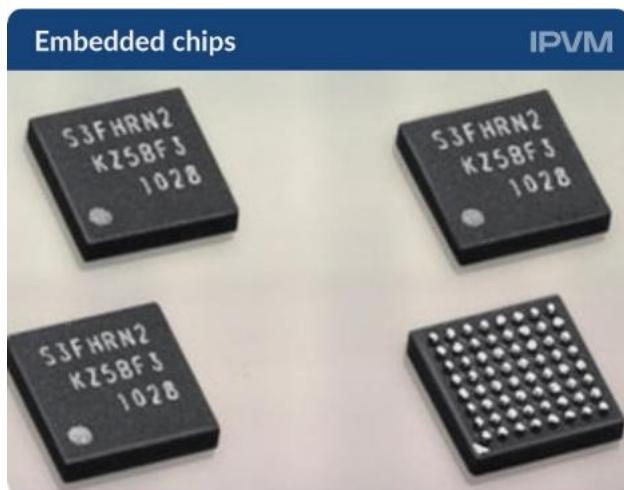


Pricing varies broadly for this form factor, depending on the expected service life for these credentials. This format can be customized according to a specific size or shape or can be furnished in adhesive-backed 'buttons'.

This form factor can be purchased from distribution for about \$0.50 - \$10.00 per piece.

### Embedded chips

Embedded chips or tags are buried in multi-function devices. The chip may be actively powered, and often this type of credential has more than one function. [NFC, or 'near field communication' chips](#) are an example of this format.



Pricing for this format is usually done in OEM component part lots and is not relevant for discussions of public purchases.

## Mobile Credentials

With mobile credentials, instead of bringing a card, clamshell, or fob at a reader, the user flashes a phone or activates an app and the door is unlocked.



Based on the rather personal value of phones, the idea that they accompany users like keys, wallets, or ID cards and they are not easily lost or misplaced makes them eligible for access control.

Mobile credentials generally range in price between \$5.00 - \$10.00 per credential, but different 'mobile' types may be no extra cost with a respective system.

However, the phone or mobile device itself has a cost. Mobile phones, even inexpensive ones, are roughly 20X - 40X the cost of a card. And the cost of maintaining a phone is much higher, requiring frequent recharges and software updates while a card remains very inexpensive and essentially free to maintain once issued.

If a card breaks or is lost, the employer reissues a \$0.50 - \$10 piece of plastic, where if a phone breaks or is lost, someone must pay hundreds of dollars to replace it.

## Applications

We find that certain form factors of credentials perform better than others in certain situations.

We provide the following application guidelines based on our field experience:

- *Picture IDs*: Cards are great for facilities that also require picture IDs. Easily worn and unobtrusive, with a low cost of issue and maintenance. Printed images are sensitive to scratching or scarring, but will still function behind a clear protective sleeve.
- *Field Use*: Clamshells are ideal for workers in the field or shops. Durable construction will not bend or break easily. Can withstand moderate abuse well.
- *Demanding Environments*: Key fobs are the best option for highly demanding or abusing environments. Resilient to shock or thermal abuse. Small size makes pocket storage easy.
- *Tools / Machines*: Not typically used as stand-alone credentials, stickers or tokens can be discretely mounted to many surfaces. Useful for applying credentials to tools, machines, or other types of credentials like metal keys.
- *Phones and Devices*: Embedded chips are most used as component parts in other devices. Never used as a stand-alone credential, but useful for integrating access control credentials in devices like cell phones.
- *Parking Garages*: As noted in [Vehicle & Long Range Access Reader Tutorial](#), in most vehicle access applications traditional readers and credentials must be supplanted by UHF based or long-range versions, so windshield stickers and tokens become primary choices.

## Hack Your Access Control With This \$30 HID 125kHz Card Copier

You might have heard the stories or seen the YouTube videos of random people hacking electronic access control systems.

The tools that claim to do this are available widely, including at eBay for just \$30 [link no longer available].

We bought one of these cheap gadgets, shown below:



Find our full test results, including a demo video of how easy it is to do, how widely these cards are deployed, and what steps you can take to cut the risk.

### Easy HID Card Copies

Our demo video below shows how the [\\$30 copier](#) can be used in seconds to spoof HID 125kHz formatted access cards:

[Click here to view the 125kHz HID Card Copier / Cloner / Hack video on IPVM](#)

In our test, we copied multiple 125 kHz formats and tested them on multiple readers. While very cheap, the card copier did not malfunction or create corrupted copies in any of the 15+ cards we copied.

### The Big Risk

Indeed, to access control systems, these copies look identical to legit cards. The screenshot below, for our test shows that multiple copies are indistinguishable from the HID factory original:

Time of event	Source	Event topics
04/26/2017 19:28:34	Axis-00408cecb58c AccessController	Access granted to users with credentials (Door 1 Entrance, , IPVM 59849)
04/26/2017 19:28:33	Axis-00408cecb58c AccessController	Access granted to users with credentials (Door 2 Entrance, , IPVM 59849)
04/26/2017 19:28:23	Axis-00408cecb58c AccessController	Access granted to users with credentials (Door 1 Entrance, , IPVM 59849)
04/26/2017 19:28:22	Axis-00408cecb58c AccessController	Access granted to users with credentials (Door 2 Entrance, , IPVM 59849)
04/26/2017 19:28:46	Axis-00408cecb58c AccessController	Access granted to users with credentials (Door 1 Entrance, , IPVM 59849)
04/26/2017 19:28:45	Axis-00408cecb58c AccessController	Access granted to users with credentials (Door 2 Entrance, , IPVM 59849)

The risk is that unauthorized copies can be made and used to gain access, with no outward sign or record of being a duplicate.

### Formats Matter

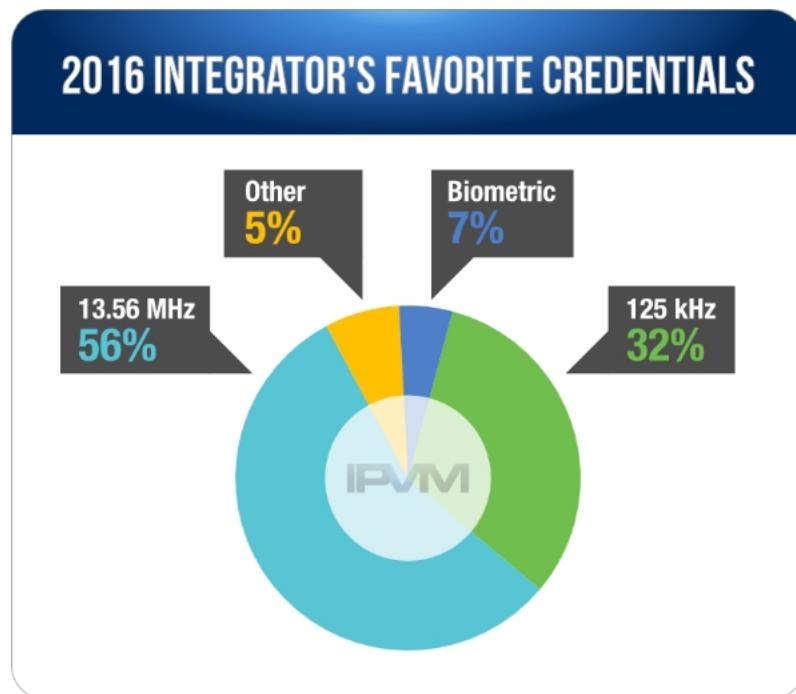
One specific caveat to this test: not all card types and formats are at risk. This particular tool can be used to copy 125kHz card types, including popular HID Prox, ISOProx, and Prox II formats, and several others commonly used in access control such as EM4100 and AWID formats.

Specifically this tool cannot copy any 13.56MHz 'Smartcard' formats like [HID iClass](#), or [DESFire/MIFARE varieties](#). One of the [major differences between those formats](#) is 13.56MHz formats are encrypted and the data they hold must be first decoded by the companion reader with a specific 'key' value, otherwise the information they transmit in open air is heavily hashed and obscured.

However, most 125kHz formats are simply not encrypted at all. This means the process of copying them simply energizes the card, and stores the information it broadcasts. Card details are stored on the card exactly as the system uses them, so sensitive card numbers and facility codes are easy to pull from thin air.

### Vulnerable 125 kHz Common

Despite the risks of unsecured 125 kHz cards and fobs, they are commonly used and even preferred by many installers and end users. In our [Favorite Access Control Credentials 2016](#), those vulnerable types command 32% of the favorite votes:



Indeed, these credentials vulnerable to copiers are still used in tens of thousands of systems, with millions of issued credentials circulating every day.

### Cheap & Easy To Get

The copier we tested was purchased for \$30 shipped [link no longer available]. Overall, the price of the unit tested was slightly higher due to the configuration of copying HID formats, but units as low as \$10 [link no longer available] can be purchased to copy basic EM4100 formats alone.

The kit we purchased was shipped with several blank re-writable keyfobs, but were not a suitable blank format needed to copy HID cards. So we bought a box of HID compatible card formats (T5557) for \$0.35 cents each, for a total test package costing less than \$45.

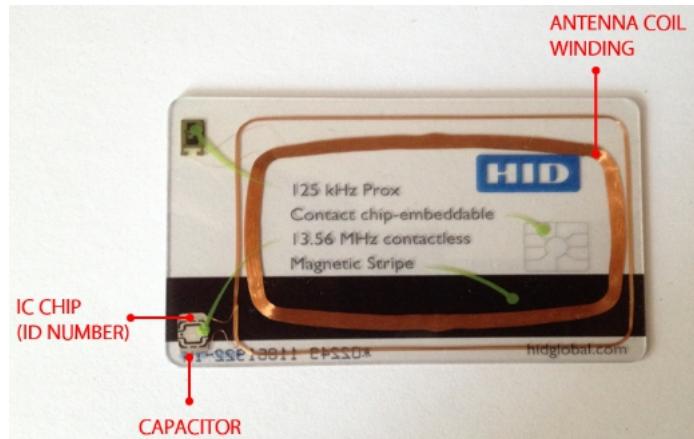
The chilling lesson is these products are very inexpensive, readily available, and sold by multiple vendors eager to ship next day with no questions asked to anyone, crook or honest.

### How It Works

The device used to copy the cards works much the same way as normal card readers, with transceiver coil, power supply, IC chip, buzzer and even LEDs components shared by both:



Given the principal operation of contactless card readers, the copier excites the coil and delivers power wirelessly to the card, which then momentarily stores energy and then uses it to broadcast card details back to the copier. The image below shows a transparent example of a card, revealing all these components:



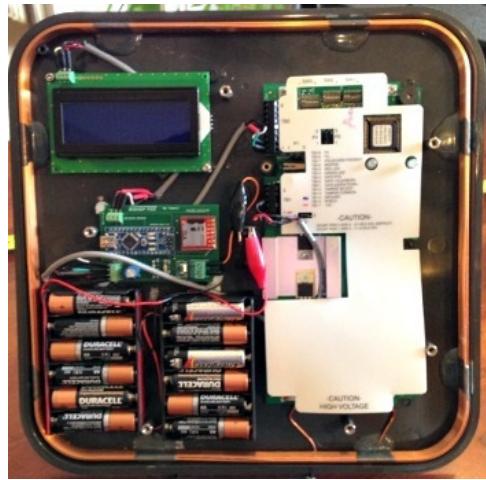
The copier includes a small amount of memory to store those details, and then pushes them to a blank card, writing them permanently as a copy.

### Near Contact Required

One particular factor of this unit are cards to be copied must be held close to the copying antenna to work, a distance of less than 1". This is somewhat a benefit to cardholders, because someone bent on stealing and spoofing card details must be very close to do it.

However, the time needed to steal the information is fast - less than 5 seconds, and it is conceivable that someone could have card details copied and stolen without realizing it, especially in crowded groups of people.

But the method used by this device is available in other forms functional at longer distances - some claiming 5 feet range or more and often using modified [off-the-shelf long range readers](#):



These longer range copiers are much more expensive (\$500+ vs. \$30), physically larger, and require more power than 2 AA batteries. However, carrying the components covertly in a backpack or briefcase means that those stealing cards can just blend in better with crowds.

### Mitigating This Risk

So what can be done to prevent this exploit? The most straightforward step is to discontinue using HID (or any) 125 kHz cards, fobs, and readers and switch to encrypted and hashed 13.56 MHz formats. For more details, see our [Hackable 125kHz Access Control Migration Guide](#).

Given current pricing, the higher frequency types are more expensive, but only a modest 15% - 25% more, and frequently offered at pricing the same or under the less secure 125 kHz types.

## Vulnerability Directory For Access Credentials

Knowing which access credentials are insecure can be difficult to see, especially because most look and feel the same.



Even insecure [125 kHz types are still widely used](#), and using 13.56 MHz smartcards is no guarantee the format has not been hacked.

We take a deeper look at:

- Why To Stop Using 125 kHz Formats
- Which 13.56 MHz Formats are Uncracked (So Far)
- The Cracked 13.56 Types Still Widely Used
- Why No Formats Are Uncrackable
- Thousands Are Working On Hacks
- Wiegand Side Attacks Used Too
- High Technology Skills Needed
- Steps To Defend Against Hacks

We cover these points inside.

## **125 kHz Riskiest of All**

While the vulnerability of specific 13.56 MHz formats is mixed, older 125 kHz are highly vulnerable to pragmatic copying with cheap and widely available components. We covered the risk in our [Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#) test, and then how to address the vulnerability with the [Hackable 125kHz Access Control Migration Guide](#).

### **Common 125 kHz Formats Are Insecure**

The list of vulnerable, unencrypted 125 kHz formats used in access is substantial, easily reaching into millions of credentials still in use daily. The common formats include:

- [HID Prox](#) (discontinued, but still widely available as a generic)
- [HID ProxII](#)
- [ISO ProxII](#)
- [Indala](#)
- [EM 4100/4200/4300](#)

### **Formats Not Yet Cracked**

The list of popular access formats currently not claimed as hacked is small and contains three main types:

#### *HID iClass SEOS*

HID's latest 13.56 MHz format has yet to be proven and confirmed as cracked using commercial tools.

HID has recently changed the default 'factory key', and as noted in [HID Mobile Tested](#), is pushing and encouraging users to use non-default client-specific (MOB) keys for all products, further tightening security of SEOS version credentials.

### *MIFARE DESFire EV1 (announced 2006) Cracked?*

This specific NXP 13.56 MHz format has been widely adopted outside North America, by non-enterprise access control vendors, and with less-expensive Asia-sourced access credentials and readers, and uses 128-bit AES encryption for onboard card details.

Claims of EV1 exploits have been distributed at red team/pen tester conventions, but the mode of attack has been exploiting mass transit passes, with exploit teams unaware or unconcerned about potential access hacks, but appearing valid for access too:

[Click here to view the New Attacks On The MIFARE DESFire EV1 video on IPVM](#)

For most distributors and access credential resellers, EV1 version product has been replaced by EV2 version credentials even when not overtly identified as EV2.

### *MIFARE DESFire EV2 (announced 2016)*

This 'next-gen' NXP format claims to offer multiple advantages related to how information is structured on the credential but does not incorporate security improvements.

In general, readers designed to use EV1 can also read EV2, although the way information is read and the formatted is different by access systems.

To date, no cracks/claims of exploits have been distributed and EV2 version DESFire is considered secure.

### **Formats Surprisingly Cracked**

The current status of exploits is not always realized by integrators and end-users. Two formats still used in many of systems have been hacked, but unknowingly sold as 'secure' by access professionals:

### *MIFARE DESFire Classic*

Though [NXP confirmed MIFARE DESFire Classic was exploited](#) in 2011, this has not been widely recognized in the PACS market, with many users assuming the 13.56 MHz encrypted format is safe.

However, the method of extracting unhashed security keys prompted the company to discontinue production. The format is still available from aftermarket vendors.

### *HID iClass Elite (non-SE/SEOs Formats)*

The effort of extracting 'keys' from HID's original 13.56 MHz format takes multiple readers and cards and was publicized heavily in the '[Heart of Darkness](#)' crack.

Once achieved individual credential information can be decoded on all cards. HID still sells these vulnerable credentials, although the most recent SE/SEOs format use a different format and multiple layers of encryption to prevent similar exploits.

### **No Formats Are Uncrackable**

Similar to claims of 'unpickable' or 'unbumpable' locks that are often exploited given time and exposure to the public, no credential formats should be viewed as 'uncrackable'.

Given the widespread interest from hackers and hobbyists looking for notoriety in breaking formats essentially 'keeping the doors locked' in countless sites, efforts to hack them are ongoing and relentless.

No access user, installer, or consultant should regard formats permanently secure, and planning for [Multi-Factor Authentication](#) and possible migration is prudent.

## Cracking Encrypted Formats Is Highly Technical

The equipment and skills needed to crack encrypted formats typically use analytic bench instruments that require software development, electrical engineering, and debugging lines of code.

One of the most popular commercial RFID hacking tools, the open-sourced [Proxmark3](#), has this disclaimer on the intro wiki:

It should be pointed out quite early that the Proxmark3 is not really for beginners. If you are not already fairly familiar with electronics, embedded programming, some RF design and ISO standards, this device will probably bring you more frustration than anything else ! Users that do not understand the basic principles behind RFID may have difficulty using the device.

For users looking for the most powerful tools, they should not expect a 'point and click' card copier, but rather a kit of components that include processors, antennas, and firmware that must be integrated together for access credential copying:



Only for older unencrypted 125 kHz formats, are cheap, ready-made, and easy to use copiers available, like the [\\$30 unit 125 kHz copier](#) we tested with confirmed success:



However, not all 'point and click' copiers are risks to access systems. For example, we tested a [Smartcard \(13.56MHz\) Copier](#) that did not work with common access formats, despite its claims of copying advanced, encrypted formats:



### Another Attack Vector: Weigand

Almost every access system is vulnerable to the risk of Wiegand copying when skimmers are installed in the reader. The card information they intercept can then be used to create identical copies of valid cards or to inject valid Wiegand signals in systems bypassing readers entirely.

However, to install these chips, physical access and modification of equipment is needed.

For example, one of the most commonly used methods of extracting encoded keys from iClass readers involves physically wiring a harness or splicing the output connection, and Wiegand Sniffers are installed the same way:

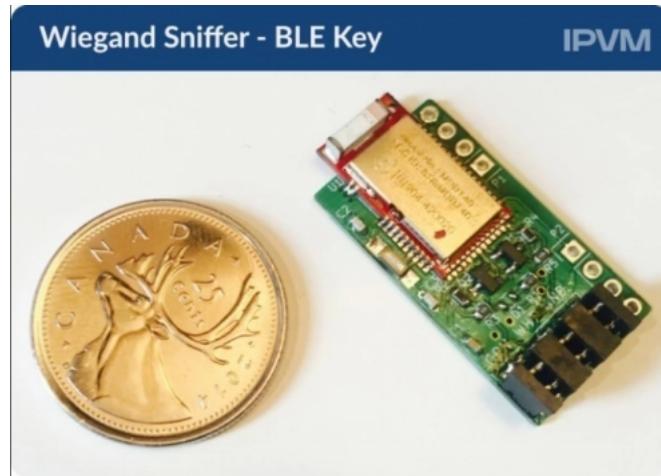


For many access systems, the visibility and time needed to use this method on a door significantly mitigates the risk, as the effort would be easily detected by authorities.

The time required for many methods often takes hours of processing. Some methods may take as few as 5 minutes (with the [Proxmark III](#)), while others take multiple hours or even days (with the [PN532 based RFID cracker unit](#)).

### **Wiegand Sniffer Chips**

For example, [the BLEKey](#), installation takes about 60 seconds, can be done from the public/unsecured side of the door, and is undetectable by the system and system managers.



The video below shows how these skimmers are typically installed:

[Click here to view the BLEKey Install video on IPVM](#)

Wiegand sniffers are easy and inexpensive to get, with kits typically [running ~\\$35 - \\$50 online](#).

#### Cracks Often Difficult To Field Execute

One key observation is that with the high skill and devoted energy need to crack credential formats, the biggest risk to electronic access control of spoofing and copying cards still takes time.

Granted, the \$30 125 kHz copier can be used in seconds and semi-covertly, so those formats should be avoided. But for 13.56 MHz formats, even those already hacked, hours of time, multiple keys, and physical modification of readers is often required.

The most pragmatic defense against hackers: maintain tight administrative control of user keys, 'turn off' lost keys promptly, do not reissue credentials, and keep sharp eyes open for tampering to installed readers and controllers.

## The Exploit Community Is Large

Similar to the 'locksport' community of hobbyists interested in picking mechanical locks, there are thousands online who actively participate and contribute to hacking access credentials.

One of the bigger forums where these users gather is the [Proxmark Developers Community](#), with thousands of users and hundreds of posts every month, where collaborative sharing of exploit progress and methods for multiple formats (including iClass, MIFARE, Legic, and UHF credentials) take place.

Other freely available, open-source resources are easy to locate. Multiple exploit projects can be found on Github, a large and often freely collaborative source of niche applications. While there are many relating to credential exploits, an example few are:

- [ColdHeat's iClass Cloner Project](#)
- [DESFire / NFC Relay Attack](#)
- [iClass \(Legacy\) Card Copier](#)
- [Mifare Classic Offline Cracker](#)

## Private Efforts

- [Milosch Meriac's 'Heart of Darkness' iClass Crack](#)
- [K. Chung's RFID/iClass Exploit Blog](#)
- [Brad Antoniewicz Open Security Research Blog](#)

# Cracked 125kHz Access Control Migration

Despite being one of the most popular credentials, 125 kHz credentials are easily copied and [insecure as we showed in our test results](#), video embedded below:

[Click here to view the 125kHz HID Card Copier / Cloner / Hack on IPVM](#)

However, changing to more secure credentials is not always a clear path, and doing it can cost thousands of dollars for even smaller systems.

We cover the most common migration paths and examine the pros and cons of each, so you can help choose the best path forward.

This guide covers:

- The 3 Most Common Migration Paths
- Pros & Cons of Each Method
- Biometrics Option
- HID Global Formats More Costly
- 13.56 MHz Read Ranges Shorter
- Changeover Cost Is The Biggest Factor

## The Major Risk

The root cause of the problem: the most common 125 kHz RFID formats used in access are completely unencrypted, so copying them is just a matter of a few seconds and takes a few dollars. Given the vast number of these insecure credentials in everyday use, the risk that threats are able to enter your facility undetected is a real issue worldwide.

## Three Migration Paths

The solution is straightforward: stop using 125 kHz credentials. Given that newer, higher frequency versions include encryption and stringent hashing of card details while resulting in minor usability changes makes them a logical replacement.

However, there are a number of options for migrating formats, each with varying costs and timelines for upgrades:

- Update Cards & Readers Immediately
- Install Multi-Function Readers, Gradually Replace Cards
- Install Separate Readers, Gradually Replace Cards

Below, we examine each method in depth and weigh the pros vs. cons to help rationalize which path is best for specific systems.

### HID Global Formats More Costly

One big consideration when migrating away from 125kHz formats is deciding which 13.56MHz format should be adopted in its place? The two most common options today come from two different vendors:

- [MIFARE/DESIRE \(NXP\)](#)
- [HID Global iClass/ iClass SE](#)

In general, HID format iClass is more expensive on a per-reader and per-credential basis compared to MIFARE/DESFire. The source of the cost difference is largely one of licensing, as all HID product is licensed, if not manufactured directly, by HID or their parent Assa Abloy. In contrast, the non-HID formats are 'open use' and essentially open for any manufacturer to build product meeting spec with no licensing cost.

The actual pricing difference between either vendor greatly varies based on individual part numbers, but the cost difference typically ranges 10% - 40% less for non HID products. However, especially in North America, support, project/account pricing, and product availability can be better for HID who retains significant market share in that market. Elsewhere in the world, NXP-based formats may be more popular, and pricing/support may be more favorable.

For detailed contrast between the two vendors, see our: [HID vs NXP Credentials](#) post.

### **13.56 MHz Read Ranges Shorter**

Cost is not the only difference between frequencies. Maximum read range length also is significantly different, with the lower frequency 125kHz format covering longer distances. While the maximum range is not a typical factor for wall mount or mullion mount applications where cards pass less than 4 inches away from the reader, using high frequency 13.56MHz formats cannot read at ranges needed for parking garage or vehicle gate applications.

For example, many [125 kHz long range readers](#) reach up to 24" with standard non boosted credentials, but their [13.56 MHz counterparts](#) only reach 18" and have warranted HID to sell a [different UHF format](#) credential and reader system instead for that application.

### **Pros & Cons of Each**

Breaking down the three options, the most secure and fastest but highest cost and system impact method is immediate replacement of both 125 kHz readers and user cards, while the least expensive but potentially slow and most vulnerable method is simply mounting a 13.56 MHz reader aside existing units and begin rotating new cards to users as needed.

The best mix of low cost, meaningful security improvement, and low system impact is to use a replacement reader that can scan multiple card frequencies and formats, often called 'multi-function' readers. This chart shows the trade-offs:

Method	Execution Speed	Security Benefit	Cost	System Impact
Replace Immediately	High Urgency	High	High \$\$\$	High
Use Multi-Function Readers	Low Urgency	Medium	Medium \$\$	Medium/Low
Install Dual Readers	Not Urgent	Low	Potentially Low \$\$	Potentially High

In the sections below, we describe each step in depth.

### One: Replace All Cards & Readers Immediately

This migration path is the most costly, but it closes the security gap the fastest by wholesale replacement of all system readers and cards at once. Eliminating production use of 125 kHz credentials means that the exploit risk disappears, but such a drastic plan requires both available budget and careful coordination of replacing existing 125 kHz issued credentials with new replacement 13.56 MHz types.



In general, a single 13.56 MHz reader can cost \$150 - \$250 and a single card often costs \$5 - \$7 before additional installation, configuration, and card printing costs, so even a smaller system with less than 8 doors and 50 users can run into the thousands of dollars, and large enterprise/multi-site systems can cost multiple tens of thousands.

In addition to the cost, instantly changing all the readers means existing credentials are not valid, so staging and planning a cutover often means preparing and issuing new credentials beforehand. And long-range applications may need to be re-engineered entirely.

As a result, the 'replace everything at once' migration is typically only used in smaller systems where the cost and logistic issues are muted.

### **Two: Install Multi-Function Readers, Gradually Replace Cards**

This migration path is often the one used, but costs and planning can still be difficult. Like the first method, option two requires wholesale replacement of all readers to a new hybrid type supporting both frequencies at once. Often called 'multiclass' or 'multitechnology' readers, these units can read either credential frequency and multiple formats.

Using this type of reader means that issued credentials can be replaced on a gradual basis rather than all at once, often delaying a big budget hit and logistics problem of replacement credentials on a programmed schedule.

While the cost of these readers is often higher on a per-unit basis compared to a single technology 13.56 MHz-only unit, the premium is modest at 10% - 15%. The price difference of replacing readers can still cost thousands, but spreading out the expense of wholesale credential replacement, even at the risk of supporting unsecure 125 kHz formats for months or years more, is acceptable for many security managers.

### **Three: Install Dual Readers, Gradually Replace Cards**

The third option is often the least expensive, but requires disciplined execution, careful system planning, and often creates eyesores where used: install a new reader next to the old one.

Cost of single-tech readers is often less than multi-function/multiclass units, and they can be installed without logistical disruption of the existing readers and cardholders.

However, installing contactless readers near each other, even when they use different frequencies, can impact read range performance of each unit. Placement so units do not cancel each other out or otherwise interfere with each other is often a field trial exercise.

If performance is not an issue, appearance may very well prove to be. Mounting dissimilar readers side by side often creates an aesthetic issue and looks bad, existing 125 kHz and new 13.56 MHz models:



Moreover, door controller hardware may not support more than one reader input, and checking, configuring, and perhaps even additional licensing of the system may be required.

However, the expense of this method may prove smallest if no other factors complicate dual reader installation, and migration to new credentials can be done with no great urgency, only whatever risk is deemed acceptable in continuing to use 125 kHz technology.

### **Considering Biometrics Instead**

For some systems, the opportunity to upgrade may consider other credential types entirely, like biometrics. While the cost of finger, palm, and iris scanners have decreased over the last decade, the cost of those reader types are typically more than 13.56 MHz counterparts, and they often require substantial outlays for user enrollment and user training on how to properly use the new readers.

Aside from these significant 'soft costs', there are often engineering or operational issues that complicate clean transitions such as vehicle or garage applications, outdoor perimeter openings subject to bad weather (and user clothing barriers like gloves), and in many circumstances additional contactless 13.56 MHz credentials are readers are implemented in certain areas regardless.

Because of the high cost and difficult operational issues, migrating from 125 kHz to biometrics is uncommon, although generally adoption of those credentials offers a high security option against future copying or credential misuse.

### **Changes Cost Money**

In all but the smallest access systems, budgeted cost generally limits how fast migration happens. End users and security managers often are forced to weigh the risk of 125 kHz products against the cost of migrating from it.

For many years, the risk was perceived as too minor to warrant spending money, however, the emergence of cheap easy copiers has changed and amplified the risks. Security managers should now consider the difficulty of getting unauthorized duplicates for 'high tech' 125 kHz cards as easy as getting 'low tech' duplicate mechanical keys cut at any hardware or big box retail store.

### **Next Up: Which 13.56 MHz Are Secure?**

In upcoming reports, we will test different 13.56 MHz formats to see which ones are vulnerable to copying or spoofing attacks using commercial gadgets or specialized software crack tools. Look for the results of which common format is 'safe' and if some types are risky.

# Selecting Access Control Readers

Given the variety of types available, specifying access control readers can be a daunting process. However, focusing on a few key elements will help you arrive at the right product no matter which system you are using.

These factors are:

- The Basic Reader Types: Contactless, Barcodes, Keypads, and Biometrics
- Quick Overview Of Contactless Frequencies and Formats
- How Mounting Surfaces Impact Selection
- Why Establishing Contactless Read Range Is Crucial
- Awareness Of Infrastructure Requirements Like Power and Connectivity
- Protocol Support (Wiegand vs. OSDP)

We address these attributes, explain how they are different, and help users understand which reader is the ideal choice for their application.

## Credential Type

The first attribute that defines card readers are which credentials they are designed to read.

For existing access control applications, the credential type has already been established and in use. Systems in long-term service may use non-standard credential types and may require specific readers from the original manufacturer, limiting replacement options as a result.

However, modern systems are equipped to read several credential types, so taking an accurate inventory of the various formats in use is a critical step.

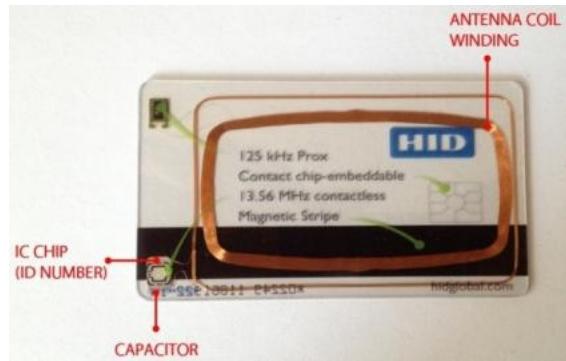
Credentials often double as picture IDs, and frequently take the form of cards and can take several forms - see our [Access Credential Form Factor Tutorial](#) for more details. The following list details the major types of credentials used in modern access control systems:

- Low Frequency, 125 kHz Standard Proximity: The most common credential types in use require the holder to wave the credential near the reader, but not make contact with it. These credentials can be read through wallets, pockets, and glass - and they are commonly used in ID cards, keyfobs, and windshield stickers.
- High Frequency, 13.56 MHz Smartcard: The newest type of card includes an onboard circuit chip (ICC) that offers higher encryption, more storage, and data rewriting capabilities. Facilities using this advanced credential often use one card for multiple systems, including logical access and payment cards.
- Barcode/Magstripe: While quickly becoming obsolete in the face of standards like FIPS-201, older access systems may still use these credentials. While convenient to program and inexpensive to issue, magstripe/barcode based credentials lack the security of other options and can be copied or spoofed easily. In addition, the durability of these credentials is not well suited for commercial use, as even mild degaussing or cosmetic scratches can impact reliability.
- Biometrics: Using physiological features belonging only to specific users is also popular. Fingerprints, palmviens, iris/retinas, and face recognition readers are commonly used by systems.
- Multiple Technology: These types of credential blend two or more of the listed types in a single credential. While more expensive, these types are the most flexible since they can be used with several different systems and can be provisioned from one database.

### **Credential Frequency Important**

For contactless credentials, a type of RF technology called 'resonant energy transfer' is used to transmit card information.

In basic terms, the principal operation of either 125 kHz and 13.56 MHz contactless card readers is for the reader to excites the coil embedded in the card/ delivers power wirelessly to the card, which then momentarily stores energy and then uses it to broadcast card details back to the reader. The image below shows a transparent example of a card, revealing all these components:



A huge risk for 125 kHz credentials is how easy and cheap it is to copy card details without knowledge of the holder. These formats are not encoded or encrypted and can be lifted by copiers with little effort.

One device used to copy the cards works much the same way as normal card readers. Our demo video below from [Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#) shows how the [\\$30 copier](#) can be used in seconds to spoof HID 125kHz formatted access cards:

[Click here to view the 125kHz HID Card Copier / Cloner / Hack on IPVM](#)

### 13.56 MHz Format Differences

The two most 13.56 MHz common options today come from two different vendors:

- [MIFARE/DESFIRE \(NXP\)](#)
- [HID Global iClass/ iClass SE](#)

In general, HID format iClass is more expensive on a per-reader and per-credential basis compared to MIFARE/DESFIRE. The source of the cost difference is largely one of licensing, as

all HID product is licensed, if not manufactured directly, by HID or their parent Assa Abloy. In contrast, the non-HID formats are 'open use' and essentially open for any manufacturer to build product meeting spec with no licensing cost.

The actual pricing difference between either vendor greatly varies based on individual part numbers, but the cost difference typically ranges 10% - 40% less for non HID products. However, especially in North America, support, project/account pricing, and product availability can be better for HID who retains significant market share in that market. Elsewhere in the world, NXP-based formats may be more popular, and pricing/support may be more favorable.

For detailed contrast between the two vendors, see our: [HID vs NXP Credentials](#) post.

### Multifactor Credential Readers

If readers accept more than one credential type to validate users, they are known as 'multifactor readers'.

These types are often required for high security applications or to offer users credential flexibility. For example, a common multifactor unit combines a proximity card reader with a keypad, so if a user forgets or misplaces a card they are still able to key a code for entry. Combination 'multifactor' units often combine card credentials with biometrics like fingerprints, retinas, or palm prints.

If a given door entry reader supports proximity cards, fingerprint scans, or a keypad code in order to be 'multifactor', two or more credentials would be required for entry, not just whichever credential option was convenient for the user to present at the time. The image below gives an example of a typical 'three factor' reader device:



With additional 'factors' come additional credential overhead, including biometric databases that often are independently maintained from the access control system. The speed that multifactor readers process additional credential factors often largely is affected by the total number of records that must be searched, and the degree of confidence a credential must have to be validated.

While most EAC systems integrate readily with basic keypad code readers, compatibility with biometric readers or high security components (eg: Hirsch Identive Scramblepad [link no longer available]) is subject to individual access control systems.

### **Mounting Surface**

Identifying the specific mounting location for the reader is the next step - while many readers are 'multipurpose', more advanced types (especially biometric combo units) are not suited for every location. In the following section, we address the most common mounting locations, and identify the variables for specifying the correct readers:

***Outdoors/Indoors:*** Like most electronic devices, the units intended for mounting outdoors must be sealed against moisture and protected against freezing. Readers are commonly available in 'potted' varieties, where the internal electrical components are sealed in resin to prevent contact with moisture. Confirming a reader is suitable for outdoor use is frequently noted as 'potted' on datasheets, which departs from industry standard IP ratings. Furthermore, the actual appearance of the reader may not change between potted/nonpotted varieties.



*Wall Mount:* The most basic orientation for mounting readers is on the wall nearby the controlled opening. While smaller readers may be designed to mount directly to drywall or masonry with simple screws, heavier readers may require additional brackets. Wiring harnesses can be directly pulled through bored holes in walls, or otherwise may be terminated in single-gang junction boxes - in this case, the reader is frequently mounted directly onto a junction box cover plate.



*Mullion Mount:* Where glass is adjacent to openings, or where control cabling cannot be fished through wall construction, a common solution is mounting readers onto hollow door frames. Because the mounting surface is typically metallic, insulating gaskets and shielded cabling may be required. These readers are identifiable by their thin profile, often only a few inches wide. Even though these readers are narrower than typical wall-mount types, they are available in the same read-ranges and offer the same multi-factor (eg: biometrics, keypad) options.



*Bollard Mount:* Readers used for gate/parking lot applications are frequently mounted on metal or concrete posts outdoors. These devices typically need longer read ranges than door mounted types, since the credential can be feet away within an automobile or windshield mounted. While these readers are typically connected to access controllers the same as other readers, they may require extra power supplies and cable shielding/grounding. These type of readers may also require the use of media converters or other expander modules to increase their communicating distance to controllers.



*Turnstile Mount:* One of the most challenging mounting locations for a reader is on a turnstile - not only are these units typically outdoors, they are frequently exposed to thermal shock, UV exposure, and impact force. Standard outdoor readers may require frequent replacement. As a result, ruggedized / vandal resistant readers are recommended for turnstile applications.



## Read Range

Determining the distance a card reader is needed to detect a credential is the next step.

Understanding the space between the reader and the controlled opening is critical - not only does it take time to physically travel from a reader to open a door (especially with wheelchair accessible openings), the standoff distance between a gate reader and an automobile may require special consideration.

Credential readers are typically available in three roughly defined distances. Each manufacturer defines the exact distance differently, and the range is typically influenced by mounting environment, interference sources, and line of sight. The standard breakdowns are:

- *Short*: these units read anywhere between close contact and 6" - 8", and are found located immediately adjacent to doors on mullions or walls. Power for these readers can be typically drawn directly from the controller without extra power supplies.
- *Medium*: readers in this class generally reach between close contact and 32" - 48", and are suited for use in parking lots and on bollards or posts adjacent to doors. These units feature different antenna coil configurations, consume more power than short range readers, and typically cost more.
- *Long*: units falling in this range typically work between 2 feet and up to 30 feet. Because of the extreme distance, readers in this category must be mounted with the same considerations as wireless networking equipment: physical line of sight must be

maintained, adjacent wireless systems can be sources of interference, and reader orientation is critical for credential detection.

Maximum read range length also is significantly different, with the lower frequency 125kHz format covering longer distances. While the maximum range is not a typical factor for wall mount or mullion mount applications where cards pass less than 4 inches away from the reader, using high frequency 13.56MHz formats cannot read at ranges needed for parking garage or vehicle gate applications.

For example, many [125 kHz long range readers](#) reach up to 24" with standard non boosted credentials, but their [13.56 MHz counterparts](#) only reach 18" and have warranted HID to sell a [different UHF format](#) credential and reader system instead for that application.

It is important to note that not all credential types have all range selections available. Less common credential types may not have the selection of 'long range' readers available, and credential formats commonly used in Europe may not be licensed for free use in the US, and vice versa.

## Required Infrastructure

The other factor to consider is what utility or secondary resources are required at the opening. Reader infrastructure aspects to consider include:

- *Power:* Most readers are designed to operate on 12VDC/24VDC and even PoE, but ruggedized and long range types may require different utilities. In general, readers are low current draw devices, typically pulling only millamps. Some types of 'stand alone' readers operate from battery packs and require no outside power connection.
- *Data:* Most readers are connected to controllers with UTP or 18/6 cable, but individual reader types may require non typical wire gauges or special features like drain cables or shielding. Wireless variants, typically using a point to many point transceiver system, are especially popular in low-cost and non-high security applications. Frequently, data

cabling is grounded or shielded to prevent interference from corrupting data exchange between reader and controller units.

- *Secondary Means of Security:* While not a traditional infrastructure component, an often overlooked feature is a backup method of securing the opening. Because most backup power systems have a finite battery life, and some hardware lock components cannot have backup power (eg: maglocks), a mechanical lock and key must be installed. Managing and maintaining this hardware is not expensive, but the only occasional use of these locks require a well organized and managed [key control system](#).
- *Intercoms/Cameras:* Finally, while not essential, secondary systems like intercoms and video surveillance cameras can help identify those requesting assistance or entry without system credentials. Invariably, a credential holder forgets or loses a credential and does not realize this fact until standing at the controlled opening. Having an intercom available allows security staff to communicate with a someone lacking credentials, without compromising area security by permitting access to secure areas.

### Protocol Support (Wiegand vs. OSDP)

A reader's output option must be compatible with the controller. Both devices must support Wiegand or OSDP, or direct reader interface compatibility for proper operations. Readers are only useful when compatible with the larger access system, specifically the door controller.

For many years the standard interoperable communication protocol between readers and controller has been [Wiegand](#), an interface that predates modern serial or TCP/IP communication. Since the early 1970's Wiegand was used to standardize reader outputs in a way that controllers could interpret, regardless of manufacturer.

However, Wiegand has some weaknesses that are only amplified in the modern era. Lack of encryption, unidirectional transmission, and the physical limitations on transmitted data size have been far outpaced by modern credential and access system design. As a result, a new standard protocol called OSDP is being promoted by leading access companies.

Our [Wiegand vs OSDP](#) note has deeper technical details, but the primary advantage of OSDP is better device manageability, status monitoring, and data handling than the old Wiegand protocol. At the current time, adoption of Wiegand is widespread and common, with OSDP less so. However, this is changing, with most manufacturers offering new product supporting the protocol and plans to expand it in years ahead.

[Note: This tutorial was originally published in 2014 and substantially revised in 2017]

# Multi-Factor Access Control Authentication

Can a stranger use your credentials? One of the oldest problems facing access control is making credentials as easy to use as keys, but restricting them to certain individuals.



Multi-factor authentication is used when the end-user is concerned about who can use access control credentials. In this guide, we explain the concept and the elements involved, including:

- What Does Multi-Factor Authentication Mean?
- What Benefits Multi-Factor Offers
- The Four Factor Types Available
- Which Factors Are Common For Access Control
- What Drawbacks Multi-Factor Authentication Have
- Why Single Factor Authentication Is Still Common

## Multi-Factor Authentication Defined

The concept means that more than one credential must be presented in order to gain access. However, the credentials are 'layered' in a way that they complement each other.

## Four Verification Factors

The individual authentication 'factors' cannot be all of the same types and are typically separately managed types of credentials. The 'factor groups' are commonly cited as:

- *Something the User Has:* A credential/permission granted administratively to the user. Typically an access control badge, token, or fob. Also includes a mechanical key, membership ID, or passport.
- *Something the User Knows:* Typically a code or password kept private by the user. Typically a PIN number, but also include 'Security Questions' or 'Last 4 Social Security digit' confirmations.
- *Something the User Is:* Biometric features only the user is able to possess. Typically finger or palm prints are used, but other readings possible including face recognition, heartbeats, retina/iris scans, and even gait.
- *Someone Trusted Verifies the User:* Under certain conditions, another human positively IDs and vouches for the user. This could be a manned guard or even a receptionist that grants access based on familiarity.

## Multiple Factors Strengthen Verification

When it comes to securing access, credentials play a vital role. When it comes to securing credentials and ensuring only the right people are using them, multiple factors are useful even if the separate factors are weak.

A familiar example to many are mag-stripe cards and PINs used for automatic teller machines. Each credential, when used alone, is weak and easily defeated or copied for malicious use.

However, even if machines do not support encrypted embedded chips, using the card is typically combined with a mandatory PIN.



So for ATMs, not only are debit cards required to be swiped, but PIN numbers are required to be entered. This makes individually weaker factors stronger by combining them into multiple layers of authentication.

### Multi-Factor Readers

If a door entry reader supports proximity cards, fingerprint scans, and keypad codes for 'multi-factor' support, two or more credentials would be required for entry, not just whichever credential option was convenient for the user to present at the time.

The image below gives an example of a typical 'three factor' reader device:



The factors that readers support vary. For example, this multi-factor reader from [BluBOX](#) includes biometric face and/or voice authentication instead of the more common fingerprint:



### Different Types

The actual number of applied factors vary according to an end-user's security concerns. Users simply concerned about the improper use of lost credentials may require two factors, while high-security installations may require three or more. We define and explain these tiers below:

#### Two Factors

Most often a combination of '*something the user has*' and '*something he knows*', seen as Access Control access card and accompanying PIN number. Even if the user loses the card, an unauthorized finder cannot use it to gain access unless they also know a code, which is known only to the user.



Because duplicating biometrics traits are very difficult, it is also common to see fingerprint or other physiological factors used as '*something the user is*' in two factor authentication.

### Three Factors

When identity requires an even higher level of validation, three factors are required. Most often this is a combination of biometrics, PIN codes, and access control credentials, and become significantly more costly to implement and manage than simple 'single factor' authentication.



As a result of both cost and time to use this level of authentication, it is used in critical infrastructure, military, and research facilities but not typically for commercial end-users.

## **Guard/Verification Factor**

The highest level of authentication is often seen at military and other sensitive locations, where manned checkpoints are used in conjunction with the other factors. Because this process takes the most time and is the most labor intensive, it typically is not employed unless the security risk is very high and existing manpower is available.



## **Multi-Factor Authentication Drawbacks**

Despite offering higher verification of users, Multi-Factor Authentication has drawbacks.

The biggest performance one is the additional time required to process or manipulate the additional credential. Especially for openings where high entry volumes are needed, asking each user to present just one additional factor could add more than a few seconds for each user, potentially adding up to many minutes over the course of all users.

Another potential factor is the increased price of multiple factor readers over simple, single factor types like contactless readers. A combination multi-factor reader is often \$500 - \$1,000 more than a single-factor unit costing \$200 - \$300. Over the course of even a small system with 3 - 4 doors, using multi-factor readers can increase costs by thousands.

## **Single Factor Still Common**

A majority of electronic access control systems use 'single factor' authentication, and this is sufficient for the operational security of most end-users. The single credential card or code is tied to the identity of the bearer, and all system activity (ie: entries, exits) is recorded for that person.

The traditional key remains the most common 'single factor' credential. No other verification of the bearer is required once the key has been issued. While primitive compared to high-tech electronic access credentials, mechanical keys still provide an adequate 'first layer' of security for many millions of facilities.

For these systems, using multiple factors to verify identity may be hard to justify. Because readers supporting extra inputs are more expensive, and hiring manned verification staff is overhead not easily justified without pressing circumstances, single factor remains the frequent method used. However, with risks increasing, there is an increasing motivation to strengthen security.

# Biometrics Pros and Cons For Electronic Access Control

Biometrics has been long sought as an alternative to the security risks of cards, pins and passwords. While biometrics has improved somewhat over the past decade and has some clear advantages, other problems or limitations remain. In this post, we compare the key pros and cons of biometrics.

## The Pros

Advantages of biometrics have key value in some access applications. While manufacturer marketing often blurs the claims and overstate the advantages, biometrics can offer:

- Credentials Always Available
- User Identity Verification
- High Credential Validity
- Tough Against Passback

## The Cons

On the other hand, there are operational weaknesses or risks that are not commonly realized before deployment. Some of those are:

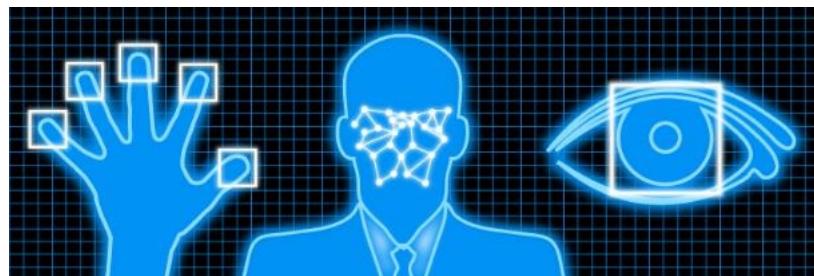
- User Unwillingness & Distrust
- User Biometric Incompatibility
- User Removal of Clothing
- User Positioning
- Injuries & Biometric Stability
- Lengthy Authentication Cycles
- No More Picture IDs

- Myth: Biometrics Are Distinctive

We explain and examine each one.

### **Biometrics Is More Than Fingerprints**

One of the contributing misconceptions with biometrics is the sheer number of technologies that are mistakenly assumed as having the same general strengths and weaknesses.



We cover the most common biometric form in our [Fingerprint for Access Control](#) post, but other common but distinct technologies include:

- Palm Prints: The outer layers of palm skin are uniquely contoured in a similar manner as fingers.
- Finger/ Palm Veins: Rather than scan the outer layers of skin, these sensors image the inner layer of capillaries just under layers of skin. These small veins are patterned in a unique way, and the deeper tissue is less prone to surface damage or contaminants.
- Iris/Retina: This type of reader takes an image of the inside of user eyes. Both irises and retinas can be used to distinguish individuals.
- Face Recognition: Taking an image of a face and measuring the size and distances between eyes, nose, mouth, and other identifying features with high accuracy and precision is becoming more common.

But there are a myriad of lesser used, but still 'user unique' biometric forms. For more, catch our [Favorite Biometrics](#) post.

## **Biometric Benefits**

In the sections below, we take a look at four advantages of biometrics. While individual methods and readers may offer distinct pros compared to others, biometrics as a general segment offer keys or minimize the risk of other credential types:

### **Credentials Always Available**

With biometrics, the user themselves are the credential, and forgetting a PIN or losing a badge is simply not a risk. Because physiological elements are indeed used to verify users, biometric credentials are available when needed and users simplify credential management by eliminating key, cards, and codes than can be misplaced or forgotten.

### **User Identity Verification**

Because users cannot lose or lend credentials for others to misuse, biometrics are useful to declare users are specifically themselves. Just as users can share cards or PINs, they cannot lend of fingerprints or irises, increasing the confidence that only authorized users are entering an area.

### **High Credential Validity**

Unlike common credential types vulnerable to copying or spoofing without notice ([Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#)), biometrics generally mitigate the problem. Cheap gadgets like the ones below cannot be used to copy biometrics:



While 'cheaper' and low-quality biometrics reader can be vulnerable to low-level spoofs, the units used in access typically employ one or several layers of [Liveness Detection](#) regardless of which biometric technology they use.

### Tough Against Passback

Biometrics essentially eliminate the risk of credential sharing as users cannot simply hand off their biometric identifiers to friends or coworkers. As covered in our [The Passback Problem](#) post, the problem is not easily solved with other credential methods and often requires advanced system configuration to stop. Biometrics often are less expensive to implement and are less complex to configure.

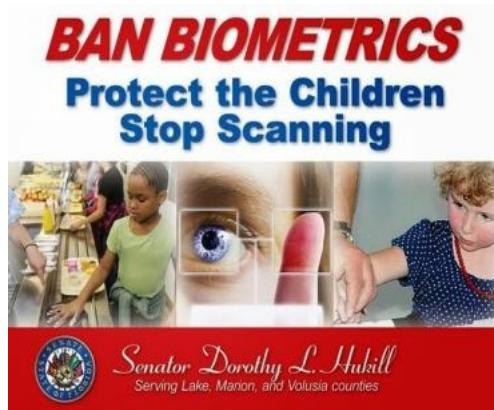
### Biometric Weaknesses

However, while biometrics may solve some problems, they amplify or create others. In the sections below, we detail seven common issues that can be showstopping problems if not recognized beforehand:

#### User Unwillingness & Distrust

Not all users are comfortable and willing to have biometric traits used as identification. A myriad of cultural, political, religious, or general lack of trust in the collecting agency or enterprise to use and protect biometric information can be a factor.

Campaigns to 'ban biometrics' in government use to identify citizens is one common hotbed of debate that often carries into private systems as well. The image below is from a [recent campaign in Florida](#):



### User Biometric Incompatibility

Quite simply, not all users may either possess or have satisfactory function of the physical biometric trait used to verify identity. Some users may lack the physical feature outright, while others may experience a 'temporary' lack of ability due to injury or infirmity. Even a biometric as common as fingerprints assume that all users have working, healthy fingers to authenticate on, and other methods of credentials must be provided for when they do not. This typically results in using multiple credential systems regardless.

### User Removal of Clothing

Another key hindrance for biometrics is the assumption the environment or location they are used will experience no user variation in the biometric trait being measured. This is often not the case, as something as simple as users wearing gloves in cold weather can be a major hassle to remove for fingerprints, or sunglasses for iris/retina scanners, or hats in rain, and so on.

### User Positioning

Not all biometrics are suitable for use in every situation, and are often less flexible than 'traditional' keys, cards, or PINs. For example, reading fingerprints while users are seated in

vehicles is highly problematic due to the physical reaching and hand positioning needed, while simply scanning a contactless card is much easier.



Complying with [Disability Laws, ADA and Access Control](#) can be difficult to adapt for all users, especially those who have mobility or ambulatory issues.

### **Injuries & Biometric Stability**

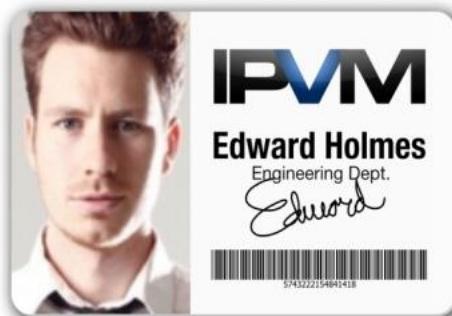
Relying totally on a biometric trait can be shortsighted for multiple reasons, when physiological changes due to aging or injury are common. For example, collagen elasticity and volumes degrade over time, so even 'unique' features like fingerprints change over the course of years, and sometimes even disappear or become negligible to read. Other factors like eye mobility, gait patterns, or even facial structures can change over time. User enrollment of biometric features is often a perennial, if not annual, task.

### **Lengthy Authentication Cycletimes**

While waving a badge or punching in a PIN can take seconds, properly registering a biometric can take much longer, even a minute or longer if retries are needed. For high-volume entrances, multiple card reader openings can handle hundreds of users per hour, but a biometric reader like fingerprints may handle a fraction of the needed total as every user must present a specific digit in a specific way every time.

## No More Picture IDs

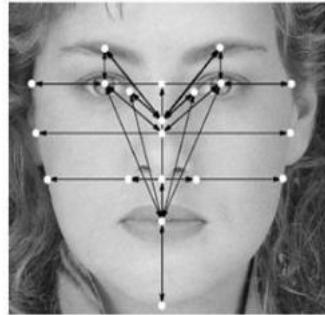
Finally, one factor not typically realized is which other ID factors are given up by adopting biometrics. While full color picture ID pictures are often printed on the same card as a contactless card and then subsequently carried around user necks on lanyards for quick visual identification, that media is forfeited when adopting biometrics and must be redundantly reissued.



## Myth: Biometrics Are Distinctive

One of the biggest errors users make when adopting biometrics is assuming all users will be enrolled uniquely and no one will be mistaken for someone else. This often results in unwelcome surprises, because any biometric is only as 'unique' as the number of sampling points collected and used.

For example, while a fingerprint or iris may indeed be unique, it may take twenty or more data sampling points before it is classified as 'distinct' in a database. Other users may have similar biometric signatures, with the same distance between features or similar (but not exact) physical traits, especially in large user databases.



In many cases, the 'confidence interval' of reading biometric features or traits requires configuring the reader or system to spend more time collecting data. The increased read time can greatly impact read efficiency and slow down user volumes passing through an opening, but will gather more information about the user, increasing the 'distinctiveness' of the biometric credential.

# Fingerprints

Users can lose badges, but they never misplace a finger, right?

The most common biometric used in access are fingerprints, and it has become one of the most trusted credentials used for access.



However, the biometric has limitations, often is more costly, and is not typically used as the only credential in access.

We examine the biggest considerations and factors for using fingerprints:

- The four factors that matter to fingerprint use
- Fingerprint reader Pros vs. Cons
- Why fingerprints do not typically replace other credentials
- Fingerprint readers typically cost more
- The three common fingerprint sensors used in access
- Why Scanning time varies
- Which specific environments are ideal for fingerprints
- Which tough environments are not a good match
- Fingerprint readers advantages over mobile access

## Fingerprint Application Barriers

Barriers exist to adopting biometrics, including fingerprints, such as:

- *Higher Cost*: Fingerprint readers typically cost more compared to 'simple' commodity contactless credential type readers.
- *Multiple Credentials Needed*: In most cases, fingerprints are not reliable enough to be used as the lone credential, and must be paired with a secondary PIN or card credential.
- *Scanning Time*: Scanning is not instant, and takes time. More accurate reads take more time, and matches in large databases can take many additional seconds compared to traditional credentials.
- *Reader Environment*: Not all readers are rated for use in harsh weather, dirty environments, or where user gloves for comfort or safety impact performance.

In the sections below, we examine the pros and cons of applications where fingerprint readers make sense.

## Advantages Fingerprints

Advantages of fingerprint readers have key value is some access applications:

- *Credentials Always Available*: Fingers do not get lost or stolen.
- *User Identity Verification Possible*: Because fingerprints are not general values, they often match specific users to credentials.
- *Tough Against Passback*: One of the classic problems with physical access is sharing credentials. Fingerprints greatly mitigate the risk.

## **Downsides Fingerprints**

On the other hand, if the primary desire for choosing them is convenience (ie: "I no longer need to carry a card"), fingerprint readers frequently are more problematic due to operational weaknesses or risks that are not commonly realized before deployment.

Some of those are:

- User Unwillingness & Distrust: Whether justified or not, users often doubt or are sceptical how securely and safely fingerprint data is stored and used.
- User Positioning: Not all openings are suited for fingerprint scans. Vehicle gate and outdoor openings are classic common problems for fingerprints.
- Injuries & Biometric Stability: What happens when fingers are cut, broken, or users age? Common circumstances often mean fingerprints work one day but not the next.
- No More Picture IDs: Plastic badges often are used as permanent picture ID cards, but fingerprint access does not use them at all.
- Myth that Biometrics Are Distinctive: Because full fingerprints are not often scanned, but only select points, the probability of user uniqueness varies and can be quite low if only a few points are scanned.

## **Other Credentials Still Often Needed**

Because reader quality varies, and because of frequent fluctuations in weather and the human body, successful fingerprint scans cannot always take place.

The most common workaround is that some form of backup credential is used, so fingerprint readers are typically packaged in [Multi-Factor Reader Models](#) that offer other credentialing options.

Regardless of manufacturer claims, no fingerprint reader is accurate 100% of the time. While the 'false positive' risk, or mistakenly granting access to an unrecognized finger, is low there is

potential for frustrating 'false negative' reads, or improperly scanning a previously authorized finger. In many cases, a quick redundant backup PIN or card can be used instead.

The reader below is one example of a 'three factor' reader, but products supporting two to five factors are common:



While multiple factors is often useful, they increase both reader and credential management costs.

Multiple factors also are useful for high-security locations, where the extra verification tightens access to only certain people, not just specific cards.

For many fingerprint applications, not only is a valid card or fob required, but biometric 'proof' that you are the person issued them is also cross-checked via fingerprint scan.

### Fingerprint Readers Cost More

The increase in cost for a fingerprint scanner is ~2X to 10X more expensive than an equivalent contactless reader.

Take for example the (~\$700) HID iClass RB25F compared to a (~\$150) HID iClass SE R40, a difference of about 4.5X.

In other cases, less expensive fingerprint readers like ZK Teco's FR1200 series cost ~\$250, and Suprema's Bioentry W series runs ~\$500. In general, even these less costly fingerprint units are more expensive than similar contactless card readers.

However, lower-priced models may be slower scanning fingers, have more difficulty reading some digits versus others (i.e., thumbs are easier but index fingers are more difficult), and maybe Wiegand only (not offering high-security OSDP).

Even when weighing the additional costs of credential cards (between \$1 - \$8 each), the contactless option may be significantly less expensive.

### **Three Common Access Fingerprint Sensors**

The sensor types used in access differ for the types used in general consumer devices. The three types more typical to access are:

- Optical / Thermal
- Contactless
- Conductive

#### **Optical / Thermal**

Most fingerprint access readers use optical or thermal sensors. In general, optical sensors are more common, although performance and prices are nearly the same.

This class of reader often costs more than other sensor types, but scans a finger on a sub-dermal level, leaving it less likely impacted by dirty skin and surface cuts or scrapes.

When users place their finger on the sensor, the sensor collects an 'image' of the finger, which is sent to a processor for comparison to a library of images. The end result of this process results in vastly more accurate reads, but requires the sensor itself to remain protected from harsh weather.

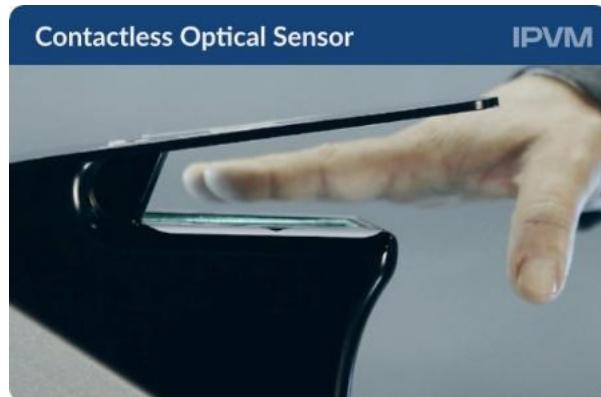


In general, one finger is read at a time and must be placed in contact with the sensor. Pricing ranges from \$200 to more than \$2,000 for these units.

### Contactless

One of the biggest issues with most fingerprint readers is that throughput is low and only one finger is read at a time, potentially becoming a big bottleneck for busy access openings.

Contactless optical scanners solve this issue, often reading multiple fingers 'on the fly' without users even breaking stride.



However, a big downside to these readers is cost, with tabletop units starting at ~\$5,000 and stand equipped high throughput models running ~\$15,000 or more.

## **Conductive**

This less expensive type of reader takes up less space, less power, and is widely used in consumer grade electronic devices and is less common for commercial access readers.

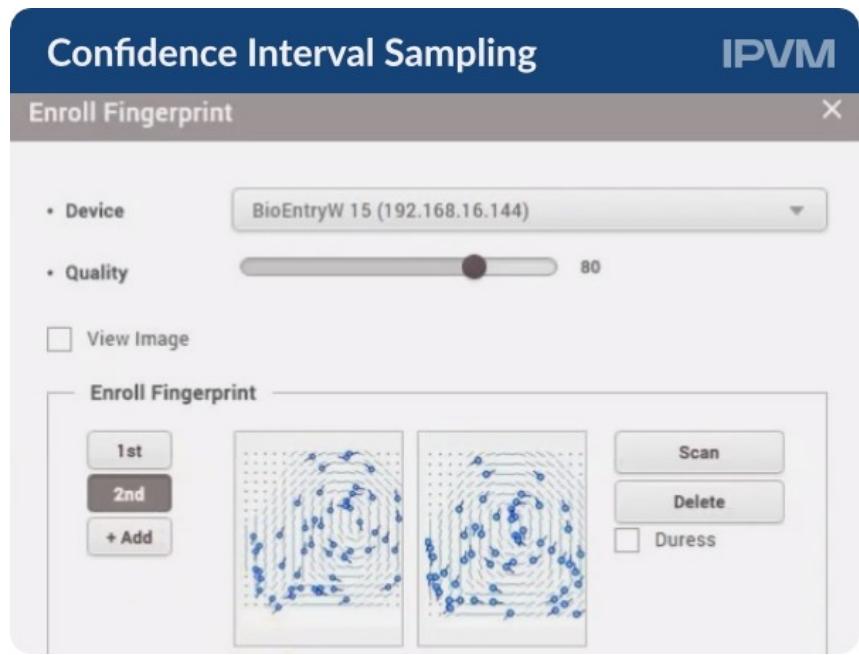
As individual fingerprints make contact with the strip, the individual features of a fingerprint make contact with the strip and register a unique 'combination'. While enrollment of an individual fingerprint is easy, the sensor is very sensitive to changes to the print, and even materials as benign as hand-lotion prove to interfere with successful reads.



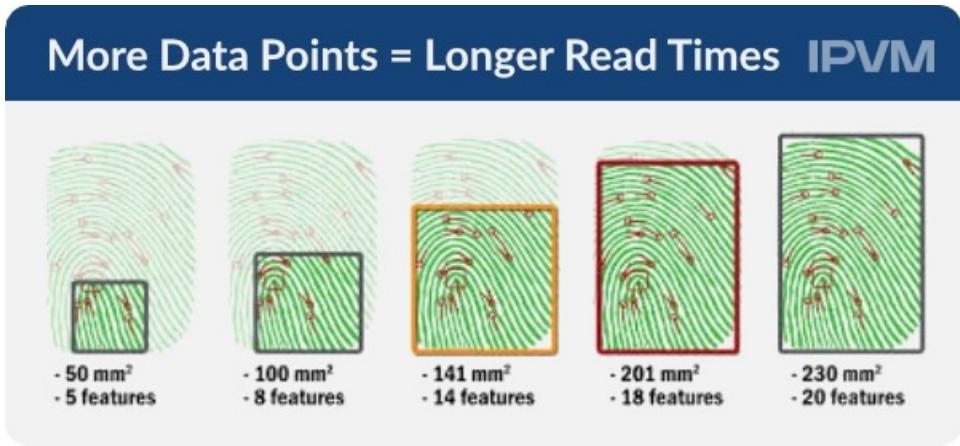
In general, conductive sensor models start at ~\$45 each but are often limited in how quickly they read prints or how many prints they can read per minute.

## **Scanning Time Varies**

Fingerprint sensors scan individual prints at a fixed number of locations ('points') and then store the characteristics of those individual sampled points as templates to compare subsequent finger scans. 'Fingerprint matches' or identity verifications are made when subsequent scan data points match up with templates, but the templates do not contain 'whole print' details.



The larger the fingerprint scan area grows, the more processing time is required to match credentials. Because the basis of biometric credentialing is taking a 'read' and comparing it against a 'known' library of records (or even just 1 user record matched on a card), the length of time a read takes to register grows too.

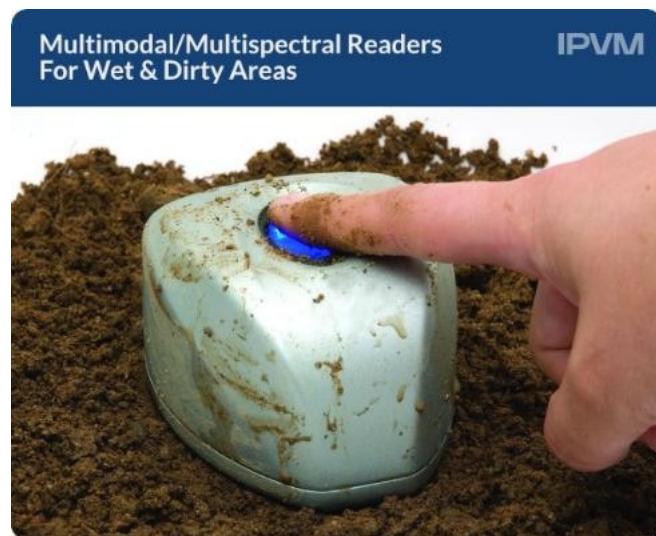


The processing time is often not substantial and less than two seconds, but overall delay tolerance tends to be much shorter when a user is standing at a locked door, potentially outside in cold or dark environments, compared to the near-instantaneous process of reading and comparing a credential card.

## Environmental Limitations

Not only do the readers themselves require protection from outside weather, fingerprints themselves require similar protections.

Circumstances like dirty hands, cuts and scrapes to finger skin, and the age of the finger bearer all factor in how easily and accurately the print is read. Likewise, readers installed in wet or dusty environments face operating problems.



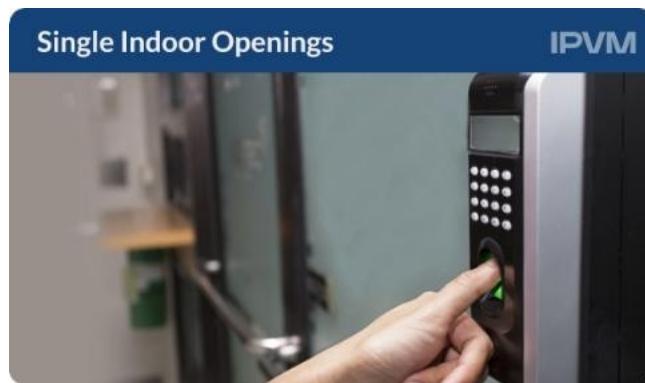
Aside from direct environment factors, there are 'indirect' considerations as well. For example, everyday accessories like gloves need to be removed in order to read a print. While a small consideration, when used in cold or sterile environments asking users to remove gloves before entry is a usability problem.

In contrast, simply flashing a plastic badge not susceptible to surface dirt, moisture, and without need to expose skin to the weather is advantageous, and most proximity style readers are available in 'potted' varieties that do not add significant cost while making them resistant to harsh weather.

## Most Common Fingerprint Applications

Given the special considerations for fingerprint readers, overall use is still low compared to card and fob readers.

In most cases, fingerprint readers are good fits for single door, indoor openings like offices or individual rooms that have a lower throughput of many users needing access at once and that are protected from weather.



For most controlled openings, traditional credentials are not a major hindrance to users, and there is weak justification to 'fix something that is not broken' given the high relative cost of fingerprint readers.

Because fingerprints and readers alike are subject to environmental factors, they primarily are used in 'high security' indoor applications where 'multi-factor' credentials are important.

## Special Applications

However, credentialing based on fingerprints have popped up new applications for the equipment. Among the 'uncommon' applications we have found:

- *Fitness Center / Gym:* Members check-in based on fingerprints, replacing the old and potentially lengthy process of manually being admitted.

- *Childcare Facilities*: In order to retrieve children, a user must scan a fingerprint that matches the 'approved to pick-up children' list. This function is especially important given custody of children is a contentious legal issue for many people.
- *Self-Service Kennels*: One application we are familiar with permits access to drop off and pick up housepets based on fingerprint ID.

### Fingerprints vs. Mobile Access

Two access technologies with high interest are biometrics, like fingerprints, and mobile where users replace their cards with smartphones.

In general, if users are using their phones for access, mobile readers do not support fingerprints too. For example, in our recent [Mobile Access Shootout](#), none of the readers we tested included fingerprints or even had the option to be fingerprint readers.

However, in many cases, the technologies are used together as smartphones often include a fingerprint activated unlock.

The main advantage of mobile access relies on users having smartphones present, while fingerprint readers require no device.

For high-security deployments where user phones are prohibited or where traditional access credentials have a higher risk of being stolen/copied, fingerprint readers (especially used in multifactor authentication deployments) are more valued.

# Fake Fingerprints - Liveness Detection Solutions

One of the biggest concerns with fingerprint readers is how easy they can be fooled. While biometrics are typically more difficult to steal or fake, headlines still break news of fake fingers or stolen prints being used to fool sensors.



For this reason, many access control fingerprint readers include live finger or liveness detection that checks the finger being scanned is authentic.

We examine the four common methods (tissue reflection, heartbeat detection, dermal electric resistance, unnaturalness analysis), what HID, Morpho and Suprema use and why you need to beware of ambiguous claims.

## Stealing Fingerprints To Spoof Identities

The root cause of the problem is that while fingerprints are unique, they can be copied or used without permission. Throughout the years, various methods of stealing prints, by complicitly [casting replicas of finger tips](#), using [gummy bear candy transfers](#), super-glue capture of latent prints [link no longer available], or even using cadaver fingers have been reported.

While the effort of producing someone else's print takes more effort than stealing a card, fob, or key, the risk is the same - unauthorized people will gain access to sensitive areas they do not belong.

## Four Common Methods

While fingerprint reader manufacturers frequently add liveness detection methods, they do not always explain what they are or how they work. In general, the number and type of methods a manufacturer include vary but typically fall into four different categories:

- *Tissue Reflection*: The most common method (sometimes called Multispectral Imaging) typically uses IR light to examine the reflected contrast of a finger's skin. This method relies on the fact that normal, healthy skin reflects IR light in a consistent way that looks different if dead or covered by synthetic material. Especially for optical based sensors, this check is done at the same time as the fingerprint is 'read', so there is no delay during the read.
- *Heartbeat Detection*: One of the strongest methods uses a high optical sampling rate to detect the momentary, rhythmic swelling of capillaries coursing with blood. This impulse corresponds to a beating heart, and without it present the scanning attempt is ignored. Being both reliant on hardware and software makes this particular method one of the more expensive options for manufacturers to use.
- *Dermal Electric Resistance*: For conductive type of sensors, healthy human skin carries a small but consistent electrical resistance. If a finger is presented and the sensor is unable to confirm typical skin resistance, it is invalidated. Even in low cost conductive strip models, this liveness check is common, but it may not be reliable in wet or cold environments that change the density of skin and blood in tissue.
- *Unnaturalness Analysis*: This method alone is the weakest, as it relies on software checks alone to determine authenticity. This method compares a print against typical characteristics of a [fake or spoofed attempt](#). Based on sensor checks like blurred, abrupt or sharp edges, blank print voids, or atypical clarity of the print, if the quality of the read falls beneath a certain 'authentic' range, the print is disregarded as fake.

Given the wide number of readers in the market, a unit without Liveness Detection can [cost \\$100](#), while a unit that layers several methods can cost 10X more. The addition of Liveness Detection is just one aspect of these units that drive price higher, along with sensor type, integration support, and environmental performance of the reader.

## Liveness Methods Used

To combat the risk of fake or spoofed prints, many commercial fingerprint scanners and readers add checks to confirm they are real. Below is a list of 'liveness detection' or 'live finger detection' on access fingerprint product specsheets:

- [Lumidigm/HID Global](#): Uses heartbeat detection and tissue reflection to validate fingers are real.
- [Morpho](#): Depending on the reader, Morpho uses tissue reflection, dermal resistance, doubled up with unnaturalness analysis.
- [Suprema](#): Uses a number of unnaturalness detections to determine if prints are faked by determining if they are copies.

In general, these companies implement more than a single method at once on readers- a key point in catching the wide array of potential fake/spoofed print exploits.

## Beware Ambiguous Claims

Not all 'liveness detection' methods are equally effective. For example [Apple's Touch ID](#) was almost immediately fooled (upon release) by a copied fingerprint spoof. Apple updated the sensor with 'liveness detection software and algorithms' (unnaturalness analysis) in subsequent models. However, the [same spoof method proved effective again](#), even after these updates. In the case of Apple's fingerprint sensor, spoofed or faked prints are still a risk with software methods alone.

In general, detection methods that use hardware and software both are better performing (ie: Heartbeat, Dermal Resistance, and Tissue Reflection). Take note of which methods manufacturers cite they use, and if software-only (like Unnaturalness Analysis) or unclear, be wary.

## Mobile Access Control

One of the biggest trends in access for the last few years has been the marriage of mobile phones and access cards. But how does this work?



Based on [our mobile access control shootout](#), we examine:

- BLE vs NFC vs Apps comparison
- Why many access systems use multiple methods
- Mobile pricing compared
- Mobile access OEMs are common
- Limited reader model selection typical

Plus we detail factors that may limit mobile's appeal for some users:

- Cards & Fobs Are Inexpensive
- 'Bring Your Own Device' (BYOD) Can Be Awkward
- Ongoing Service Billing
- Awkward or No Picture IDs
- Battery Power Limitations

## **Mobile Credentials Convenience**

Using mobile devices as credentials to open doors has a big cool factor.

In many cases, the phone may not need to be unlocked or app activated in order to open a door, with user phone proximity or twist gestures being enough to send readers user credential data.

Instead of bringing a card, fob, PIN, or fingerprint at a reader, a user flashes a phone or activates an app and the door is unlocked.

Based on the rather personal value of phones, the idea that they accompany users like keys, wallets, or ID cards and they are not easily lost or misplaced make them good potential card replacements.

## **Three Major Mobile Methods**

In terms of formats, three common methods of mobile credentials are used in access:

- BLE (Bluetooth Low Energy)
- NFC (Near Field Communication)
- App Based Credentials

## **Mobile Credential Format Comparison**

Structurally which method is used makes a big difference for overall mobile access performance.

In general, access manufacturer data sheets will detail which/how many methods are available with their product, with each method having different limitations and benefits.

The breakdown below shows the major differences between types:

Mobile Credential Format Comparison IPVM			
	NFC	BLE	App Only
Range	Typically <9 inches, ~3 feet max	Typically 150 feet max	Unlimited based on cellular or Wi-Fi range
Battery	Needs power to program NFC chip, but power optional afterward	Needs power to activate onboard radio every time used	Needs power to activate onboard radio every time used
Frequency	13.56 MHz	~2.4 GHz	Cellular/Wi-Fi
Mobile OS Support	Android No iOS	Both Android & iOS	App Specific, but both Android & iOS is common

For example, notice the difference in Range between the three formats. While NFC range is short (typically less than 9 inches), the range for BLE is longer at ~150 feet, while App systems essentially have ranges only limited by Wi-Fi and cellular connectivity.

In other cases, which method is used impacts reliability too. For example, with HID Mobile, using BLE is less reliable for connecting to the reader than NFC, and because different phone types may limit which method is options used, overall user experience is often determined by which mobile access method they use.

### Many Access Systems Use Multiple Methods

In order to minimize the weakness of a particular format, many mobile access vendors incorporate multiple mobile methods in their systems.

For example, [HID Mobile](#) uses both BLE or NFC, while [Openpath](#) uses all three. The available methods depend on how mobile is integrated into the access platform, as is the case with [Nortek BluePass](#) and [ProdataKey \(PDK\) Touch IO](#). Though they are the same underlying product, PDK integrates using App and BLE vs. BLE only for the Nortek version.

While NFC or BLE readers also support RFID credentials, they usually communicate directly with the [door controller](#), or use Wi-Fi to communicate to the reader.

## **BLE (Bluetooth Low Energy)**

BLE is the most common method mobile access method, included in almost all mobile phones and mobile access products.

A key benefit is that BLE licensing costs are free or low cost compared to NFC, and manufacturers expend little money to produce BLE compliant gear regardless of volumes sold.

In terms of weaknesses, BLE requires device power to transmit, so dead phone batteries are a showstopper and often require backup credential methods like cards, fobs, or PINs to be used.

BLE has become the most common method of remote credentialing, given reliable engineering standards definition and low/no app licensing costs. Many consumer-grade products like [August](#), [Kevo](#), and other smartlocks use BLE to connect credentials.

## **NFC (Near Field Communication)**

NFC inclusion in phones is mixed, with Android phones adopting standard implementations, but Apple/iPhones using proprietary [Apple Pay](#) that does not work with mobile access.

In terms of strengths, NFC sidesteps the limitation of phone power to use a credential. Once an NFC chip has been encoded as an access credential, it can be used in a passive mode and field energized by readers, a feature neither BLE or Apps offer.

While common outside the US for applications like banking, library cards, and mass transit, NFC use is still fragmented inside the US and generally BLE is more widely used.

## App Based



A third, but less common, method uses an app to trigger a door unlock directly.

The app method first was seen in several consumer-grade offerings like [Lockitron](#), but has expanded into commercial platforms like [Brivo](#), [Farpointe Data](#), [Kisi](#), [Openpath](#), [Proxy](#), and others.

The image at right shows a 'Tap here to unlock' button available as a [Farpointe Data Conekt](#) app option:

Using this method, phones use Wi-Fi to communicate with readers or directly interface with networked door controllers.

This interface may require customer networks to allow remote access via VPN or through firewalls, etc. to door controllers.

### Pricing For Mobile Access Control

The cost of adding mobile to exist access typically requires newer readers (often replacing older ones) and a software / licensing cost.

Pricing for readers typically range ~\$200 - \$350 each.

Software / licensing cost ranges significantly:

- One time software license fee: This is typically the least expensive overall typical option with vendors like Farpointe Data and Nortek generally charging under \$10 per device, one time only.
- Monthly software license fee per reader: OpenPath and Proxy charge a monthly fee per reader of \$20. Given a common ratio of 10 devices (or more) per reader, this is an effective cost of a few dollars per month per device.
- Monthly software license fee per device: This is typically the most expensive overall option with vendors like HID and Lenel generally charging \$6 or more per device per month.

At the high end of mobile licensing, with \$70+ or more per year per device, credential costs can increase 10x or more compared to conventional physical credentials that range from \$2 to \$8 each and, on average, last at least a year, if not multiple years.

### **Mobile Access OEMs Common**

Often access control vendors use private labeled/OEM'd providers for their mobile access offerings.

For example, the access brands below use these suppliers:

Mobile Access OEMs Common		IPVM
Brand	Supplier	
AMAG Symmetry Blue	WaveLynx Ethos Mobile & Unikey	
Lenel BlueDiamond	3miliID	
Prodata Key Touch IO	Nortek & Unikey	
ZKTeco KR500BT	Farpointe Data Conekt	

Even commonly recognized access brands ones, often buy their mobile from other vendors, and which features a mobile system has may vary based on licensing and integration, not technical limitations.

### Limited Reader Model Selection

An overall limitation of mobile access is that only a few readers are compatible, which may limit placement and even how the reader is connected to a door controller via Wiegand or OSDP.

The comparison image below from our shootout shows the variation in physical reader size, and common application areas like mullion mounts may not be possible based on which product is used:



In some cases, like with [HID Mobile](#), a number of form factor, card credential format support, and Wiegand vs. OSDP connection options are available because the entire HID SE reader line is mobile compatible.

However, options are significantly limited with a reader like [Nortek Blue Pass](#) with only one size, 125 kHz and Wiegand-only model available.

### Management & Other Practical Problems

Incorporating and managing mobile access is not simple for commercial access control.

A range of credential and access control management issues crop up that are not typically factors with traditional credential methods. These include:

- Cards & Fobs Are Inexpensive
- 'Bring Your Own Device' (BYOD) Can Be Awkward
- Ongoing Service Billing
- Awkward or No Picture IDs
- Battery Power Limitations

### **Cards & Fobs Are Inexpensive**

Mobile phones, even inexpensive ones, are roughly 20X - 40X the cost of a card. And the cost of maintaining a phone is much higher, requiring frequent recharges and software updates while a card remains very inexpensive and essentially free to maintain once issued.

If a card breaks or is lost, the employer reissues a \$10 piece of plastic, where if a phone breaks or is lost, someone must pay hundreds of dollars to replace it.

### **'Bring Your Own Device' (BYOD) Can Be Awkward**

In most cases, employers will not be buying employee phones. Therefore, 'Bring Your Own Device', or asking users to leverage their personal phones for commercial uses presents numerous problems.

Issues can range from how enterprise network security is maintained, to whether or not phone owners are willing to permit employer provisioning and perhaps management oversight on personal devices.

### **Ongoing Service Billing**

Another fundamental issue is what happens if the phone bill is unpaid?

Do service interruptions remain the responsibility of employees, even if they cannot enter work buildings as a result? Or will employers manage payment?

Either way, the question leaves a new policy to be established not otherwise needed if mobile credentials are not used.



### Awkward or No Picture IDs

Unlike physical cards that are often printed with the user's picture, name, and other identity details like QR Codes or magstripes, these are hidden or obscured from sight with phones.

Picture IDs add a factor of identity verification for those carrying cards, where at a glance others can match the picture on a card to the person presenting it for access.

Unfortunately for mobile phones this is made difficult by unlocking phones, which require users to show other pictures or other proof the phone they are holding is theirs.

Policies like forced password or biometric unlocking for phones may be required for mobile users, and while security is increased, overall difficulty and time to access the phone may diminish some of the 'mobile access' value.

## Battery Power Limitations

Even problems as basic as battery life are issues with phones, and their ability to transact credentials compared to unpowered credential fobs or cards:



Indeed, battery power, operating condition, reliable function, and even multi-tasking demands are mitigated issues with cards.

## Mobile Access Shootout

For a detailed look at five of the leading mobile access platforms, see our [Mobile Access Control Shootout](#) where we examine the key strengths and weaknesses of each.

Catch deep testing of each of those platforms in our mobile access test series:

- [HID Mobile Tested](#)
- [Farpointe Data Conekt Mobile Tested](#)
- [Openpath Access Control Tested](#)
- [Proxy Access Control Tested](#)
- [Nortek Blue Pass Mobile Access Reader Tested](#)

# Keypads

Keypad readers present huge risks to even the best access systems. If deployed improperly, keypads let people through locked doors almost as if they were unlocked.



However, despite the drawbacks, keypads are still one of the most common choices in access today.

We examine the weaknesses of keypads including:

- Revealing Buttons
- Snooping Eyes
- PIN Sharing is Easy

We offer advice on how to deploy them securely and examine a type of keypad that overcomes glaring weaknesses.

## Operation Described

The function of keypads in access control is simple. A door or gate remains locked until the user enters a valid combination string into a nearby number pad, usually a sequence of numbers.

Most access control applications assign each user their own number, called Personal Identification Number (PIN). Unless the user enters a valid combination, the opening remains locked.

## Why Use Keypads?

If these input readers are so terrible, why do people use them? The single biggest 'pro' in using keypads is that no external credential is required. There are no cards or fobs to buy, fingerprints to enroll, and template records to manage. A user is given an access code that is presumably memorized or included in other documents, and nothing else is required.

The lack of external credentials results in a lower operating cost relative to 'credential-based' systems.

## The Problems

Despite being one of the oldest and most used access readers, keypads have huge vulnerabilities. Worse still, it takes no special tools or skills to exploit these problems. While individual units may be better, or even worse, than others at these shortcomings, the biggest problems are:

- Revealing Buttons
- Snooping Eyes
- PIN Sharing is Easy

In the sections below, we examine these issues and address how they undermine even the best access control platform and most secure locks.

### Revealing Buttons

Keypad buttons wear and collect dirt over time. This is a huge problem because only the buttons needed to gain access are the ones typically showing proof of use.

## Dirty Buttons

The reader below has buttons that pick up dirt and grime from the user's fingers. At first glance, only four buttons show this soil, but even the most inexperienced intruder would likely associate the physical location of the keypad with a common characteristic of the area, the US Post Zipcode.

Simple guessing and less than 5 minutes of challenges will open this 'secured' door. Soiled buttons, even when representing a 'random' number, reduce the potential combinations from tens of thousands to a few hundred, and likely combinations (address/phone/apartment numbers) may take seconds to narrow down.



## Worn Buttons

Likewise, wear is obvious in the example below.

Instead of grime, notice the keypad buttons are constructed of plastic that is worn off over time. In this case, guessing the most likely combinations is significantly aided by seeing the buttons most frequently used:



### PINs on Labels/Stickers

A third common weakness is labels, stickers, or etchings that note a valid PIN right in plain text:



In general, these values are shared as a matter of convenience, but users utterly mitigate any security value of the PIN at all, and the value of access control on the opening can be argued as pointless for most applications.

## Snooping Eyes

Even when evidence of prior combinations is not obvious, users can be watched entering their codes.

Unless a user is deliberate in shielding their fingers and the keypad while entering a PIN, even a casual observer can note and memorize the code. A more determined intruder may even use long-range optics or even 'exotic' thermal cameras to snoop out valid combinations:



## PIN Sharing is Easy

Even if 'passive' means of gaining a code are difficult, a huge vulnerability almost impossible to mitigate are users sharing codes outright. It may seem like an easy solution for an inconvenient circumstance, but sharing a unique PIN with just one other person means that 'access control' is lost.

Even worse are examples where valid and general codes are written on labels or stickers, adhered to the unit in plain sight, and totally undermine having electronic access codes at all:

## Configuring Wiegand Can Be Problematic

Connecting the reader to a controller may also prove challenging. The communication protocol common to most readers for many years, Wiegand, was initially developed without clear direction on how to incorporate keypad signals.

As a result, incorporating keypad inputs can be fragmented, with some controllers requiring 4-bit, 8-bit, or 26-bit values. Generally, controllers include the flexibility for these settings, but the exact values needed will vary depending on which Keypad reader is used.

## OSDP Keypads

One of the 'improvements' [claimed by OSDP](#) is that reader keypads now communicate values in standardized (but encrypted) ASCII formats.

The portion of the v2.1.7 OSDP standard defining this (4.11) is shown below:

<b>4.11 Keypad Data Report (osdp_KEYPAD)</b>			
Sent as a "poll response"			
This reply is sent in response to an osdp_POLL if there is any data in the keypad buffer. It is applied when the keypad is in default operating mode.			
Unreported keypad data is deleted in case of, or during, a communication loss.			
Reply Structure: 2-byte header, variable-length data			
Byte	Name	Meaning	Value
0	Reader Number	0=First Reader 1=Second Reader	Any
1	Digit Count	Number of keypad digits to follow	Any
2 – N	Data	Digits from the keypad buffer in the order in which they were entered.	See Below
The key encoding uses the following data representation: Digits 0 through 9 are reported as ASCII characters 0x30 through 0x39 The clear/delete/* key is reported as ASCII DELETE, 0x7F The enter/# key is reported as ASCII return, 0x0D Special/function keys are reported as upper case ASCII: A or F1 = 0x41, B or F2 = 0x42, C or F3 = 0x43, D or F4 = 0x44 F1 & F2 = 0x45, F2 & F3 = 0x46, F3 & F4 = 0x47, F1 & F4 = 0x48			

## Steps To Overcome Keypad Weaknesses

With careful attention and active management, the inherent risk with keypads can be minimized. The steps include:

### Clean and Maintain Units

Wipe away oils, grime, and even 'temporary' impacts like snow. Installing keypads inside of hinged enclosures may help, but physically inspecting the buttons, keeping them clean with a mild solvent (rubbing alcohol or ammonia), and inspecting the buttons for damage and wear will go a long way in preserving security.

However, all the additional effort results in maintenance cost not typically needed by other credential types like contactless cards or biometrics.

### **Routinely Change PINs**

One of the biggest failures of keypad is that PIN assignments never change. Over time, the user's sense of responsibility to keep the number of secure slips.

The best and most authoritative method of remedying loose control of PINs is simply to change them on a routine basis. The frequency of changes depends on the population of users, for systems with less than 100 PINs, changing twice-yearly helps refresh the value in user's minds.

### **Multifactor Authentication**

Another key method of beefing up keypad security is to combine them with more than one credential. For example, requiring users to carry both credential cards AND PIN combinations has the added effect of ensuring that neither lost/stolen cards nor shared codes can be individually used. We examine using multiple credentials together in our [Multi-Factor Authentication Primer.](#)



However, the penalty for adding additional factors manifests itself in additional time to credential through openings and issuing/maintaining secondary credentials.

### Use Scramble Keypads

Some keypads are more secure than others. A version called 'scramble pads' or 'random pads' do not display numerical digits in a predictable "1-9,0" orientation, but instead, randomize the values every time they are used. The randomness mitigates the 'button wear' vulnerability and evenly distributes wear among all buttons. Two common types are shown below:



The advantages of these units are the randomized orientation of digits each time a user punches in a code, cannot be viewed unless directly in front of the unit. However, they are very expensive (~\$900 - \$1200, compared to <\$200 for 'non-scramble' types) and not always supported by the access system.

## Hotel Access Control

Hotel access control does not work like typical commercial access control because doors in hotels are not typically directly connected to a central server.



How does it work then? How can the hotel assure that cards are used properly? We cover:

- Hotel locks not typically networked
- Why mobile key apps control more than doors
- Credential overviews and prices
- Typical hotel door lock price
- How systems protect against unapproved access
- Advantages of hotel vs commercial access systems
- Safety and security concerns with hotel access

### Locks Not Typically Networked

The biggest single difference in operation between 'hospitality' and commercial access systems is the role of the credential.

A hotel/hospitality door lock is not networked to a server to check valid or invalid credentials, rather only unlocking when a credential 'tells it' to open. The credential itself contains all decisions and data needed to activate the lock.

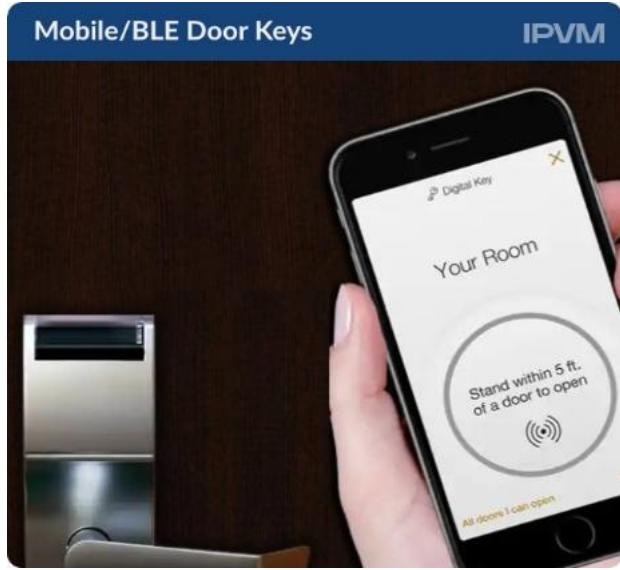


In contrast, an access system only uses the credential to initiate a request for access. The credential itself does not issue a command to open the door, it simply identifies the holder against an 'approved' dataset for entry.

By contrast, the networked portions of the controller can verify with a central cardholder database.

### **The Move To Mobile**

A significant addition to Hotel or Hospitality Access is the incorporation of Bluetooth and NFC based room keys in addition to RF-based or magstripe room keys.



The move to app-based credentials allows features that physical card keys do not allow, specifically enabling patrons to check-in and unlock their rooms without needing to engage front desk clerks.

Using mobile credentials still do not require WiFi or hard-wired networking of the door lock, and the transactional activities are managed by the app via the network connected smartphone.

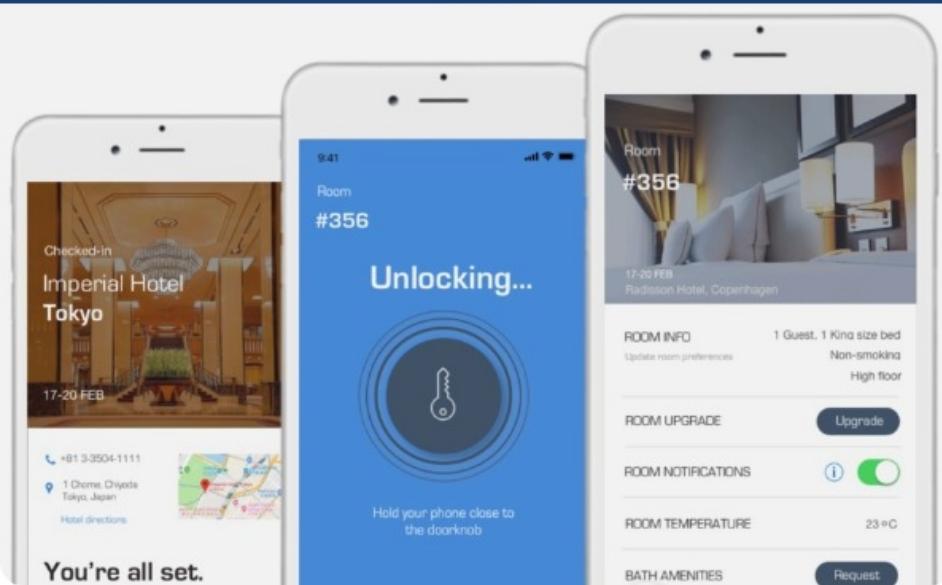
### Apps For Amenities & Marketing

With app-based credentials, other access controls and features are often made available to users.

For example, amenities like pools, gyms, or towels can be 'access controlled' via the same apps. Patrons can share door keys with others, or even meals or other consumables can be scanned using the keys and debited to the user's account during the stay.

## Digital Check-In and Amenities App

IPVM

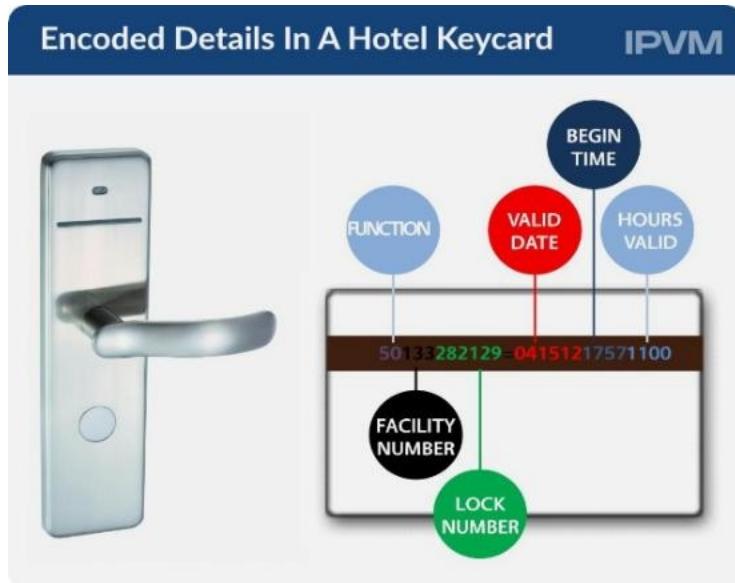


Some hotels even allow users to control room heating/cooling, phone calls, or room service calls from the app, as well as using the app to market customized rates or packages based on user app activity or even proximity to a certain hotel.

### Hotel Credentials Overview

In the hospitality industry, access control systems consist of individual, non-networked door reader/locks, a phone app, or a card programmer and encoded access cards.

In many cases, the central enrollment workstation, usually at the front desk, encodes a keycard with common access data. For mobile-based systems, the same data is passed to a door lock via BLE or NFC:



Among typical values are:

- *Function*: a number used to classify the keycard as a 'guest card', 'Master Key', 'housekeeping card', or other type of role. 'Guest cards' typically open one door, while a 'Master Key' code may open them all.
- *Valid Date/Time*: the time period a card is able to open a lock. This may also include a 'begin time' to calibrate lockset with system time.
- *Lock Number*: a unique ID value specific to the lock/room the card opens. This generally limits opening to one door per guest card.
- *Facility Number*: a unique code that identifies the particular property/floor/wing a card is encoded for. This prevents using the card for 'Room 123' at multiple facilities.

The door lock relies on the credential itself to determine when it should unlock, so the system itself is essentially not networked and each lock is 'updated' and makes an access decision only when a card is presented.

### Keycard Prices

Keycards must be cheap for these systems to make economic sense. Unlike brass door keys, keycards must be disposable or cheap enough to discard after a single-use.

The most common types are CR80 size cards that cost around \$0.20 - 0.50 per card. This standard size measures 3.375" x 2.125", the same size as a credit card, and are typically made of inexpensive PVC plastic.

In some cases, the cost of these cards are further subsidized as advertisement space by marketing incentive programs, local restaurants, or attractions nearby a hotel:



### Magstripe Encoded Cards

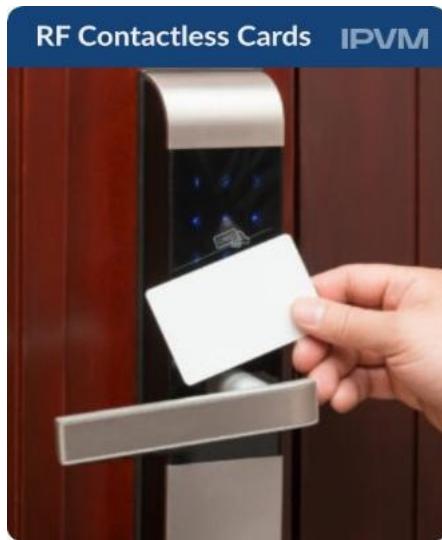
A key trait of these credentials: the data stripes on these cards are a 'softly' encoded low coercivity mag stripe compared to more permanent types of credentials like contactless smartcards.

While this may result in the periodic 'demagnetization' of these cards if subjected to even mild magnetic sources, this attribute is often presented as a security enhancement in the form of 'short service life' of the issued credential. The physical card encoding method provides the added benefit of expiring after a short time, often a few days.



### RF or Contactless Smartcards

In some cases, hotel locks support common contactless formats used in commercial access, often MIFARE and DESFire formats.



Using these types of credentials do not fundamentally change operation or management of the system, but otherwise use contactless credentials that are used in a way that most patrons are already familiar with.

### Door Lock Price

While the price of door locksets can vary greatly depending on design and finish, 'basic' units can be purchased for less than \$200 USD. Some popular models used in 'budget hotel' chains

sell for less than \$75 USD. In contrast, enterprise-grade commercial electronic access control systems often cost upwards of \$1,000 per door.

In general, door locks are designed to fit only the most typical door types using cylindrical or mortise cutouts. Unlike other forms of electronic access control, hospitality systems only work with a specific type of door and cannot be adapted to multiple types.

### **Protecting Against Unapproved Access**

A common question that arises with hospitality systems is "How does the door know when to deny my card?"

Given a normal check-in/check-out interval, this answer is determined by the 'valid date range' of access encoded on the card. When the check out date is reached, the encoded data on the card is read as 'invalid' beyond a certain point. However, for dynamic situations, like unexpected early check-outs or extended stays, employee cards play a vital role. To accommodate for these situations, it is a common requirement that cards for the housekeeping staff are 'refreshed' every day, and the 'internal' rules in a hotel door lock are updated daily when the housekeeping staff insert their cards while making their rounds.

Functionally, employee cards are not constrained by the same access rules as guest cards, and can be configured for indefinite access. However, a common feature of hotel locks is the 'mechanical override' deadbolt that disables the external card reader when thrown. For these circumstances, it is common to see a mechanical, keyed door lock in the lever that allows access in an emergency.

### **Advantages of Hospitality Systems**

The most notable characteristic of hotel access systems, compared to commercial, is they are inexpensive to purchase, maintain, and operate.

Despite the rather 'high tech' impression these systems give guests, programming a new card and handing it to a guest is easy enough for inexperienced clerks to manage, and because of their disposable nature can simply be thrown away rather than forcing 'key management' like traditional systems.

Other advantages include:

- Limited cardholder rules to program
- Easy to invalidate cards by reprogramming lock
- Can be completely 'turned off' by throwing mechanical deadbolt from inside room
- Mechanical override keys allow emergency access at all times
- Typically, door hardware logs up to 200 - 500 events allowing for forensic investigations as needed

### **Disadvantages of Hotel vs Commercial Access Systems**

However, traditional electronic access has key benefits for access management and user security that hotel systems generally don't:

- Multifactor authentication or biometric support
- Ability to program multiple access schedules and access locations
- Credentials can be immediately revoked or 'blacklisted'
- Doors can immediately be 'locked down'
- Credentials are used on a semi-permanent basis and carry multiple credentials
- Hardware is not typically powered by battery packs and is more reliable and cheaper to maintain
- Many thousands of log events stored in controllers

### **Hotel Systems Use Closed Resell Channels**

Hotel access control is not a market segment typically serviced by the security integrator.

While exceptions exist, reduced profits and high maintenance usually result in these systems being supported in-house by hotel maintenance staff.

In general, the security approach of traditional 'hardwired' access control is seen as 'overkill' and complex compared to the low cost, purpose-built alternatives found in the hospitality market.

Hospitality System manufacturers sell and install their own products, often bypassing the traditional integrator channel. This business model is justified for several reasons:

- Margins are very low, typically beneath the profit threshold an integrator will pursue.
- On the flip side of the coin, the manufacturer is able to control pricing. These systems depend on the 'RMR' of replacement keycard orders, and as a result they sell the door hardware and installation labor near cost.
- Hospitality chains typically treat 'keycard systems' as 'supply items', and would rather buy replacement products (cards, battery packs) from negotiated pricing programs from hospitality supply distributors, rather than security integrators.

## **Hotel Access Security Concerns**

Several recent incidents have magnified the risks of hotel access systems compared to enterprise access. Take this example, where a careless or clueless clerk encoded every guest card with a 'Master Key' function, essentially allowing a single guest to open every door:

[Click here to view the Rodeway Inn Guests In Gallup video on IPVM](#)

The risk described in this incident can be avoided, but not completely mitigated with hotel access systems. With a fully networked enterprise access system, such an error could immediately be corrected if made, and the door lock itself configured to simply not open or remain locked to outside users until the problem is addressed.

# Controllers & Management Software

# Access Control Door Controllers

Door controllers are at the center of physical access control systems connecting software, readers, and locks.



Despite being buried inside enclosures or hidden inside ceilings, they are a complex component that ties everything else together.

We examine controllers and their main features including:

- The three typical forms of controllers
- The primary function of coordinating access at the door
- Hardware compatibility across access management software
- Typical input devices for access, including readers
- Common types of outputs, including locks
- IP vs Serial Connected Panels
- Traditional DC vs. PoE Power
- Controller features within standalone locks

## Controllers Are Mandatory For Access Control

The primary role of controllers is linking other access components like locks and readers into a system control point, whether it is called a 'controller', 'door module', or 'access computer'. Every reader, sensor, and lock must be tied into 'the system' and the controller is where that happens.

### 3 Types of Controllers

Depending on the system, the controller is typically offered in one of the following ways:

- Enclosures
- Standalone/Appliances
- Combo Controllers

#### Enclosure Type

The most common types of controllers are printed circuit board housed in a small electrical enclosures or 'can'.



The enclosure is typically wall mounted in a closet or ceiling mounted above a door, and all wiring passes through knock-outs in the can to terminal blocks on the board.

Advantages of enclosure controllers are they available in high-density versions (32 or more doors) that connect multiple openings into a single box, unlike other controller forms that support one or two doors. These high-density configurations are often [easier to secure](#), use less wiring, and are more efficient to manage compared to locating a controller at each door.

The location of connection points inside these enclosures vary, but typically each terminal block is where individual device connector wires are installed and become usable by the system:



### **Standalone Appliances**

Another common controller form factor is as an 'appliance', or device contained in its own enclosure.

While these appliances are not typically mounted into enclosure cans, access components are connected in the same way as enclosure controllers, but into a self-contained box:



This form factor is common with small systems using single door controllers and cloud/hosted access systems.

While having the benefit of having their own enclosure, deployments using many appliances can occupy significant amounts of space.

### Combo Controllers

Sometimes the door controller is factory integrated with readers, cameras, or motion detectors in a single device:



This controller type often decreases installation labor because multiple access components are installed at one time in one device.

However, this type of architecture can be a security liability, with the vulnerable controller being mounted along with the reader on the vulnerable side of the door. As noted in our [Combo Reader / Controllers Tutorial](#), these controllers use safety wiring connectors to protect lock wires and are not typically used for high-security openings.

There are examples of 'combo systems' in the market that typically combine Intrusion/Burg alarm systems and access control. While not strictly controllers, these combo systems often tout the same advantages of using labor to install multiple system components at once.

### **Which Controller Do I Pick?**

The choice of access control management software generally drives what controllers can be selected. Many access software systems only support a limited number of controller form factors.

As a result, controller selection options are typically limited to one brand, but a manufacturer may offer a range of controller options typically sized based on the number of doors it is designed to control.

### **Limited 3rd Party Controller Options**

Access control systems often use proprietary or 'closed' controllers that function only with specific access software. Unlike cameras and VMS software, access controllers are not typically mixed/matched between different manufacturers.

While access control system controllers support is often limited, there are a few 3rd-party controller suppliers including Axis, HID, Isonas, and Mercury exist, as we cover in our [Open Access Controller Guide](#).

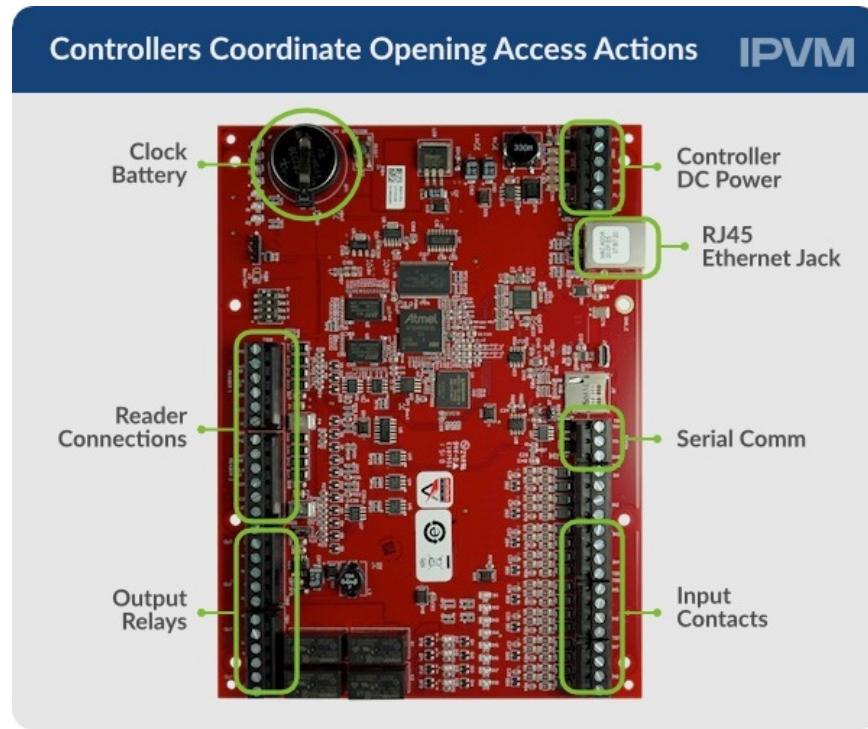
In many cases, an access brand may use controllers manufactured by another company and relabeled as their own (e.g., Mercury controllers relabelled by Lenel). While the hardware may

be technically interoperable between access software, they are often not tech-supported and unwarranted between systems (see: [Replacing / Switching Access Control Systems Guide](#)).

## Controller Functions Explained

Regardless of form factor, the features of a controller are similar.

We have marked the common controller features and 'tie-in' points between other access control components and the door controller, in the image below:



The primary features and common integrations of a controller include:

- *Networking Controllers:* How does the controller communicate with the master panel/server?
- *Inputs:* Where do devices like readers feed information to the controller?
- *Outputs:* Where are devices like locks controlled by the controller?
- *Power:* How is power handled by the controller, and how are attached devices powered?

## Networking Controllers

In most cases, controllers have RJ45 ports so they can be connected to LANs like any networked device:



The popularity of PoE and the general use of ethernet in access facilities have made IP door controllers popular.

However, serial connected controllers are common, especially in older systems. When serial connected, communication between controllers is handled via dedicated cabling that is terminated directly to control boards. Unlike an ethernet connected device, troubleshooting serial is specialized work that does not take place on an ethernet.

## Common Access Inputs

The purpose of inputs is to 'feed' information into the access system. The number and types of inputs connected to the controller vary, but all controllers accept the basic types listed below:

- Readers
- Door Position Switches
- Request-to-Exit & Safety Sensors

We examine each type in the following sections:

## Readers

The most exposed and vulnerable access control input component is typically the credential reader.



Usually, the reader is mounted on the 'unsecured' side of the opening, and potentially exposed to bad weather, vandalism, and is vulnerable to damage. For this reason, the risk of using vulnerable [125 kHz](#) and Weigand reader models has given way to more modern 13.56 MHz and [OSDP](#) format readers.

The number of reader inputs a controller supports is not always equal to the number of doors it can control. Many designers can mistakenly assume 'one reader per opening', however, high-security applications often require two readers - a 'read in/ readout' application that still only supports a single opening schedule or range of access levels.

Aside from keeping the controller secure, a detached reader is configurable according to the type of credentials being read, the mounting surface, and the read range. For more details, catch our [Selecting Access Control Readers](#).

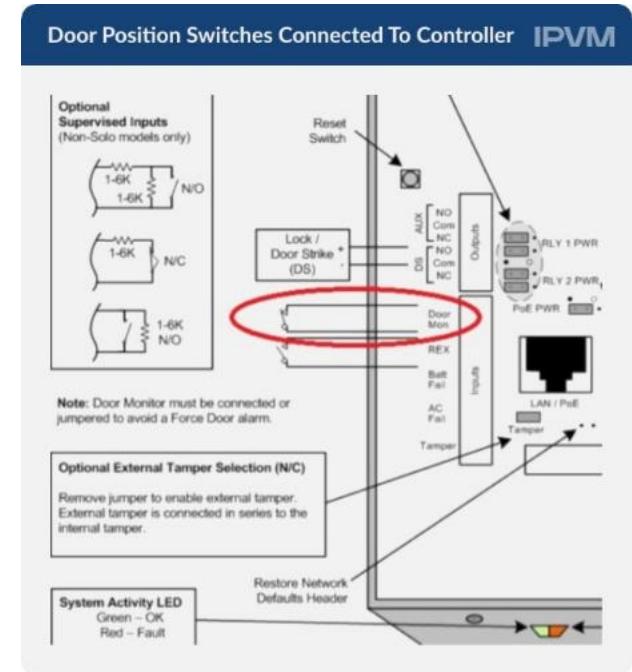
## Door Position Switches (DPS)

One of the most useful inputs are contact door closure switches, in order to determine if a door is opened or closed. Most DPS are simple contact switches that use closed or open circuits to indicate door position.

The main types of DPS are the five types below, examined in our [Door Position Switches \(DPS\) Tutorial](#):



Connecting DPS to controllers may use general-purpose inputs, or may use specifically labeled input ports called 'Door Monitor' or 'DPS' inputs:



## Request-to-Exit & Safety Sensors

These types of standard input devices "RTE" or 'Request-To-Exit' devices, use to override locks in order to accommodate free egress.

The legality of connecting these devices to the controller rather than interruptingly power directly varies, as we examine in [Access Control Request to Exit \(RTE\) Tutorial](#), but the two major types include timed 'Exit' buttons and PIR motion sensors:



## Fire System Integration

Fire alarm systems are commonly wired into controllers so that a fire alarm condition will override the locks in an emergency.

## Video Surveillance Not Through Controller

While video surveillance is frequently integrated with access control, typically video will be integrated with the access control management software, rather than through the controller.

## Common Access Outputs

Controllers drive actions for outputs connected, such as:

- Locks
- Sires/Strobe Lights
- Access Integrated Systems like Visitor Management and Vending Machines

## Locks

The most common output example is locks such as electric strikes, maglocks, and other types of electrified hardware.



The controller is the device that interprets a valid read and applies logic to unlock the door. An output signal, or relay contacts breaking power to the lock, interrupts the 'locked' state of the hardware-based on a successful credential read.

### Sirens & Strobe Lights

Controllers can also be wired to chime sirens or energize strobes based on inputs. Announcer can be wired to sound when a door opens, or lights can be wired to energize as someone passes through an opening.



### Other Systems/Devices

Like input connections, output options are endless, and anything from gasoline pumps, high-voltage machinery, and VMS systems can be triggered and controlled by access control outputs.

Common integrations using controller output ports include dispensing supplies in a vending machine (i.e.: Safety Equipment like [Personal Protective Equipment](#)) via badge scans in a vending machine, or door overrides into a [Visitor Management System](#).

Another common output integration is the triggering of a surveillance camera to record an opening every time a credential is read.



## Power Options - Low-Voltage or PoE

The type of power used by controllers is generally either low-voltage (12/24 volt) DC or [Power over Ethernet \(PoE\)](#). In many cases, extra power from those sources is passed-through the controller to power output connected devices.



As we examine in [PoE Powered Access Control Tutorial](#), passing-through power to devices is a matter of careful consideration. Not all devices are designed to be powered by the controller, and in cases like maglocks, the output power from the controller may not be sufficient.

## Controller Sizing

Physical controller size is typically determined by the number of doors they control.

Common sizes are single, double, four, and eight door models. While models supporting a greater number of doors are available, they are not common.

## Standalone/All-in-One Locks

While not strictly door controllers, standalone electronic access control locksets often feature the same integrations and control available to door controllers but tied into a package that includes the lock, network interface, power supply, and even door position switches.

Increasingly, 'wireless locks' are being promoted by access companies as the least expensive way of adding networked access control to doors difficult to reach with standard wired networks.



While the door controller component may be factory integrated into the lock, it essentially is still there performing the same functions (even equipped with the same firmware) as discrete door controller devices.

# Access Controller Software

Properly configuring [access controllers](#) software is key to a professional access system.

These devices have fundamental settings that must be configured appropriately, including:

- Unlock times / extended unlock times
- Door Hold Open Alarms
- Request to Exit Inputs
- Card Formats
- Reader / interface type
- Input / output devices
- Tamper switches

We review all of those elements including examples of configuration with Axis, HID, Hikvision and Mercury controllers, a hands-on-video, and an explanation of the importance of each element.

## Configuration Options Defined

The major settings that must be customized to every opening include:

### *Unlock Times*

Given that opening sizes and spacings are different, and locks they use need to accommodate the variation, the main setting used to adjust performance is how long a lock is powered/unpowered or unlocked. Because it takes time to register a credential and then walk to or pass-through an opening, this setting is central in making sure the opening is only unsecured long enough to allow one user to pass through before becoming relocked.

### *Extended Unlock Time*

This variation on basic unlock time is generally given to specific credential holders based on special needs (like wheelchairs) to job responsibilities (like delivery people). Users flagged with 'extended unlock' times have a longer period to keep doors open before they are re-locked or 'held open' alarms sound.

### *Door Hold Open Alarms*

Because open doors are not secure, access systems generate 'door hold open' alarms to notify operators when doors remain open for too long. If not configured, the system will not physically prompt operators to close or troubleshoot potentially risky situations.

### *Supported Card Formats*

In general, controllers need specific drivers or interfaces to properly interpret information from attached readers. While controllers almost always support [Wiegand or OSDP](#), support for other proprietary types may be available or needed by specific access systems.

### *Request to Exit Hardware*

Some types of locks (ie: Maglocks) and some openings incorporate [Request to Exit](#) devices that allow users to override door locks without using credentials. Because these devices only need to interrupt the lock temporarily, the sensors used to manage these activities are connected to the controller and not the lock directly. The controller allows an RTE sensor to trigger an unlock, but the controller also restores the lock and opening to a normal state after a short period has expired.

### *Tamper Switches*

In addition, a variety of nuisance and tamper detection inputs must be configured when, how, and who receives notifications when they happen. In general, controllers are useful for taking

simple contact closures or openings and sending emails, SMS, or even VMS alarms when someone is disturbing access equipment.

## Configuration Screen Examples

Despite the wide variety of door controllers used by access systems, the method of configuring them and even the terminology used to describe settings is generally similar. The sections below show four common controller examples:

- HID Edge EVO
- Axis A1001
- Mercury Security (EP-1501)
- Hikvision 260x Panel

These units are 3rd party models detailed in our [Open Access Controller Guide \(Axis, HID, Isonas, Mercury\)](#) note, and while totally independent of each other, configure similar fundamental variables. In most cases, the underlying management platform can always be used to configure these settings, although some web-based or standalone units let you configure them directly on hardware.

### HID Edge EVO

First, an [HID Edge EVO](#)'s settings are located under the 'Door Parameters' tab:

 **Door Parameters** \* Required

---

Edge Solo Door Name:	<input type="text" value="HID Edge Solo"/>	The name of the door.
Unlock Time (1-1620 sec):*	<input type="text" value="6"/>	The amount of time the door is unlocked during a grant access.
Extended Unlock Time (1-1620 sec):*	<input type="text" value="19"/>	The amount of time the door is unlocked for a cardholder needing extra time.
Door Held Time (1-1620 sec):*	<input type="text" value="37"/>	The amount of time the door can be held open before an alarm occurs.
Unlock on REX:*	<input checked="" type="radio"/> Yes <input type="radio"/> No	Specifies if the door is unlocked when the REX (request to exit) is activated.
Reader Type:	<input type="button" value="Card"/>	The type of reader.
Keypad Type:	<input type="button" value="HID"/>	The type of keypad connected to the Edge Solo.
Electrical Interface:	<input type="button" value="Wiegand"/>	The electrical output type for this reader.

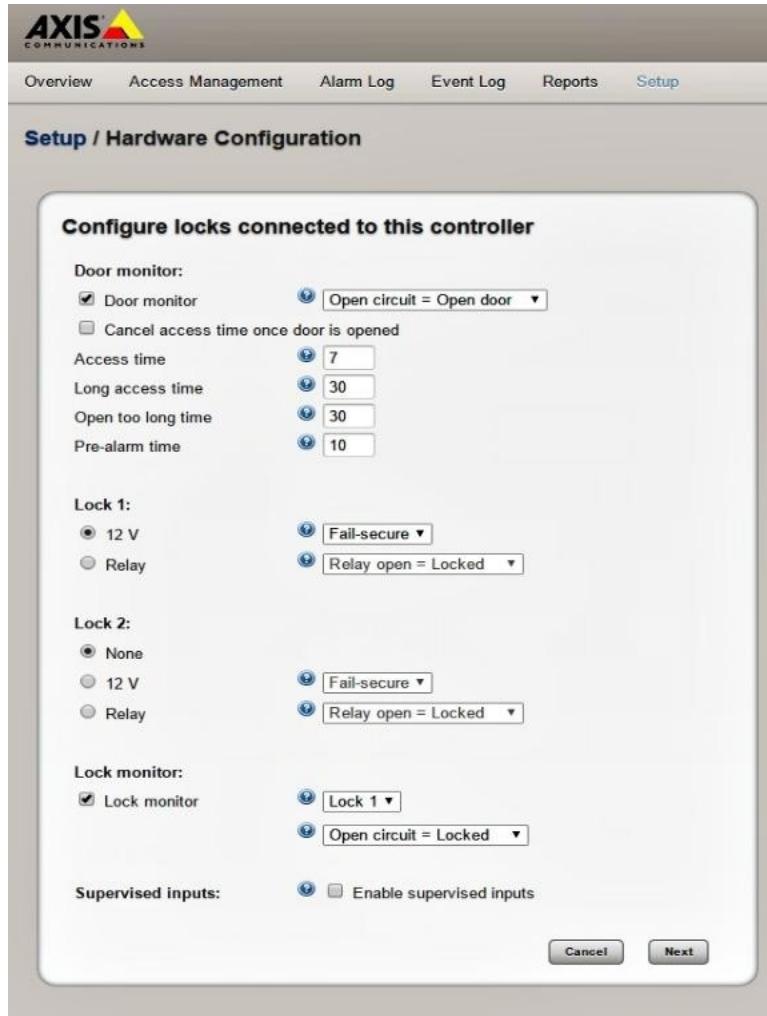
 Cancel

 Save

Note that 'Unlock' and 'Extended Unlock' times can be assigned a period between 1 second up to 27 minutes, and a brief explanation of each setting is listed beside each control. In this controller, the physical connected reader format and keypad is also configured in this screen.

## Axis A1001

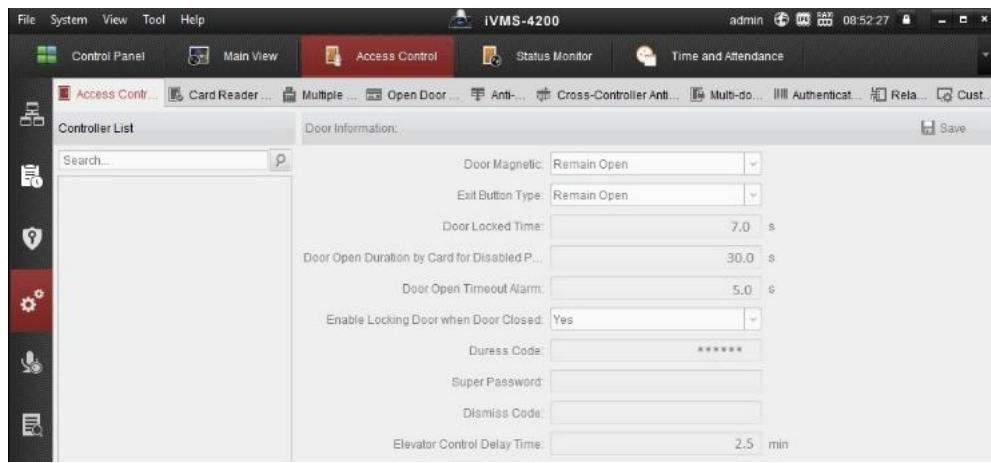
The two-door Axis controller ([test report here](#)) lists these settings under the 'Hardware Configuration' screen:



Note the same basic lock and extended unlock times are listed, but called 'Access Time' and 'Long access time' respectively. In addition, door held open (Open too long time) and nuisance (Pre-alarm time) values are also listed on this screen. Note the behavior of inputs like 'Lock Monitor' or [Door Position Switches](#) can also be configured here.

## Hikvision Access Controllers

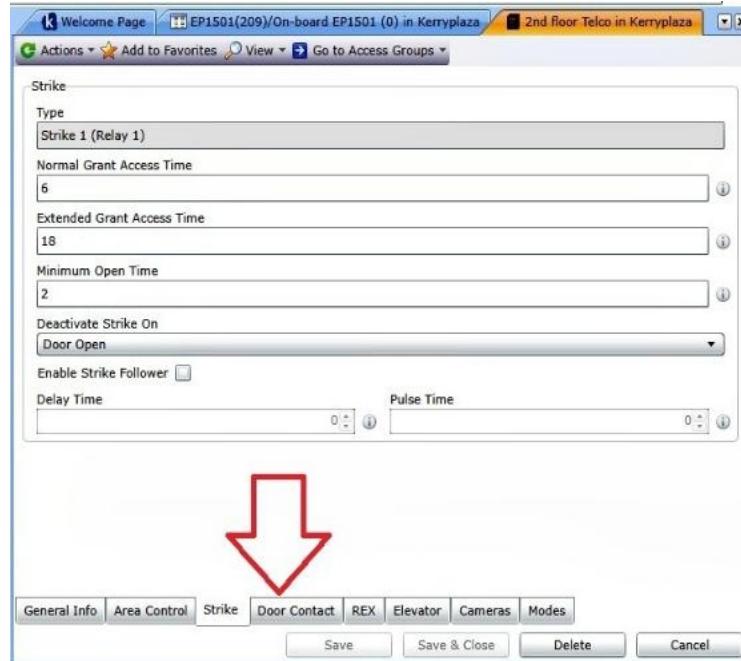
Hikvision (see: [Hikvision Access Control Tested](#)), has an interface for changing controller settings in their iVMS-4200 software:



While the label language varies, the features they control are the same as other platforms. For example, 'Door Open Duration by Card for Disabled Person' is the same as 'Extended Unlock Time', and 'Door Open Timeout Alarm' is 'Door Hold Open Alarm'.

## Mercury Security Controllers

For Mercury products, the settings determining these functions are located in the partner management software interface rather than on the hardware controller or board itself:



The arrangement and total number of controls depend on how deeply the parent software has integrated the hardware controller, but in general Mercury partners, all include base features like lock 'Access Time', extended access duration, and common input/output components like locks and door position switches.

## Practical Setting Applications

In the real world, these settings can have a significant impact on how well the access system operates.

### Unlock Times

This setting usually involves a range of times, typically seconds or milliseconds. The correct setting varies widely between opening types and even individual users. Common access-controlled openings and the typical unlock times include:

*Doors:* For 'standard' swinging doors where the reader is mounted immediately adjacent to or on the door frame, the unlock time generally is set between 5 and 10 seconds. This allows enough time for someone to scan a card, turn, and pull open a door before it relocks, but is quick enough to secure the door behind the user and require that user to rescan to unlock it.



Close readers equal shorter "Unlock Time"

*Vehicle Gates:* The range of times needed to safely open a gate and drive a vehicle through vary depending on the type of operator and style of gate. However, considering that standoff

distances can be 20 or more feet, the controller may need to close relay contacts for 60 seconds or more.



Gates need more unlock time than Doors

**Mantraps:** When doors are installed in series, or intended to close and lock in sequence, a controller (or series of controllers) must be configured to lock and unlock based on the status of other doors. For more detail on [Mantraps, see our note](#). Because a man trapped door often cannot be opened until the previous opening is locked, the "Unlock Time" maybe 5 seconds or less.

### Extended Unlock Time

**Handicap or Delivery Users:** When a credential carrier uses crutches, a wheelchair, or has a job that requires passing through an opening several times in a short period, an "Extended Unlock" time is often assigned to that user, to keep the door unlocked longer than typical for convenience. For example, a delivery person may not be able to transfer all packages through a door in 5 - 10 seconds, but a period of 15 to 35 seconds may be long enough to pass through without accidentally relocking the opening.



**Special Needs require "Extended Unlock"**

### Door Hold Open Alarms

Open doors cannot keep risks out, but if alarms sound after unrealistic durations, the access control system can quickly be ignored as a nuisance. For most openings, Door Hold Open alarms should not be configured for less than 30 seconds, and not more than 3 minutes.



However, the exact duration assigned often needs to be determined by observed use.

### Hardware Configuration Options

In addition to software configuration, some attributes depend on hardware selection also. The major factors include:

- *Number of Authentication Factors:* Related to reader type is the combination of credentials needed to open a door. For example, even basic access systems offer an option of card, PIN, or both card & PIN credentials to open a door. The decision of how many factors to use may be limited by controller support of various credential types and may require software configuration for production use. For a deeper look, see our [Multifactor Authentication tutorial](#).
- *Input/Output Devices:* The 'theoretical' range of I/O options for access may be endless, but the ratings of the relay contacts onboard the controller play a big part in how they are connected. For background, see our [Inputs/Outputs Guide](#). If a range of devices with different voltages and amperages are to be switched by the controller, the may need to be grouped, terminated, or installed in 'supervised' circuits where they are switched.
- *Onboard Tamper Switches:* In most cases, configuring a panel or enclosure tamper contact is useful for sending an alert as it occurs. Most controllers include a tamper contact or switch onboard, but setting it up for use is often optional. Software configurations, input contact configurations, or changing jumper settings are common steps required to use these tamper switches.

### **Controller and Reader Wiring Example**

In the video below, we give a brief overview of the other common configuration work done on readers - physical connection of components like readers. Many controllers use low voltage phoenix connectors to physically connect components that are controlled via the settings described above.

In some cases, the settings detailed above may not be detected or recognized for configuration until the physical components are wired to the controller. This video shows how wiring is typically accomplished via simple label call-outs or even contact color coding:

[Click here to view the Wiring A Controller video on IPVM](#)

## Open Access Controller (Axis, HID, Isonas, Mercury)

In the access control market, there are many software platforms, but only a few companies that make non-proprietary door controllers.



Recently, [Axis released a 3rd party-only controller](#) and [Isonas joined 'Openness' ranks](#), while [HID purchased Mercury Security](#).

We contrast common access hardware providers and which brands of hardware many access management systems use.

- The 3rd party offerings of Axis, HID, Isonas, and Mercury
- How their pricing compares
- Why ONVIF for Access Control Is Not A Big Factor
- A chart explaining which controllers 34 notable access platforms support
- The three factors that may complicate takeovers

### 'Open' Controller Options

In the access market, the number of manufacturers producing door controller hardware is comparatively small to the total number of vendors writing management software.

While some companies choose to produce their own proprietary controller designs, a significant portion of the market chooses to integrate with 'open' 3rd party devices manufactured by others.

For the access control market, the most widely recognized non-proprietary door controllers are produced by three companies:

- *Axis*: The company offers two different controllers, the [A1001](#) and [A1601](#). Both models are two-door controllers, but the A1601 is built with higher memory capacity, faster processors, form C relays. Both units use Axis' [VAPIX API](#), although the free embedded [Axis Entry Manager software](#) is only an option for the A1001.
- *HID Global*: Owned by Assa Abloy, HID also manufactures two series of controllers, Edge and VertX, that with a firmware update can be added to over 15+ different access systems.
- *Isonas*: The [Allegion owned](#) access hardware manufacturer [opened its line of controllers](#) to being integrated into other platforms in 2017. The company's line of combo readers/controllers are IP based and PoE powered.
- *Mercury Security*: [Purchased by HID in 2017](#), the hardware manufacturer sells only to other businesses. Mercury produces several lines of controllers and expansion modules, including the IP-based LP and EP series and [Series 3 Redboard](#) panels with a common firmware framework. [Over 35 companies](#) use Mercury designed hardware, or other hardware using Mercury's standard firmware.

These offerings compose most of the 'open' controller options in the market, but if you are familiar with others feel free to [email us](#) so we can add to our list.

### Defining 'Open' for Access

In the case of access control and the broader security market, 'Open' has a different general meaning than IT and software development use. 'Open' for access essentially means 'non-proprietary' that is potentially compatible with several systems.

This differs from 'openness' in other tech areas where 'open-source' generally means use is free, collaboration is public, and licensing (if implemented) is light and provisional.

## Cost Comparison

While pricing varies for each controller, the hardware cost alone may also be subject to additional software licensing. However, on a hardware only basis, pricing looks like:

- *Axis A1001 & A1601*: The A1001 is widely available online for ~\$500, while the A1601 runs ~\$700.
- *HID Edge EVO*: The single door controller is available from distribution with a street price of ~\$350, with options for units with integrated readers for ~\$450.
- *HID VertX*: The base controller and two-door expansion module is available through resellers for ~\$650, but total cost varies depending on which base controller and how many expansion modules are used.
- *Isonas*: The company's line of RC-04, PowerNet, and IP Bridge controllers range from \$700 (single door) - \$1,100 (three door bridge) depending on configuration of the included reader.
- *Mercury Security*: None of these products are available as direct purchases from Mercury or through distribution. Single door controllers typical range in price from \$250 - \$400, but the final cost is often heavily negotiated and drops for projects with large door counts.

## Compatibility Chart

The chart below provides a look at leading access brands, and which door controllers they work with:

	HID EDGE	HID VertX	MERCURY SECURITY HID	AXIS A1001 A1601	ISONAS ALLEGION	PRIVATE BRANDED
Alarm.com Access				●		
AMAG						●
Avigilon		●		●		
BluBOX				●		
Bosch				●		●
Brivo	●			●		●
Cbord	●	●				●
Dahua						●
DSX						●
Feenics	●	●	●			
Genetec	●	●	●	●	●	
Hikvision						●
Honeywell NetAXS						●
Honeywell Prowatch			●			●
Identicard			●			●
Imron		●	●	●		
ISONAS					●	
Johnson Controls	●		●			●
Kantech						●
Keri Systems			●			●
Keyscan						●
LenelS2			●			●
Maxxess	●	●	●			●
Milestone	C	C	C	C	C	
NLSS	●	●	●	●		
Open Options			●		●	●
Openpath						●
Paxton						●
ProData Key (PDK)						●
Proxy						●
RS2 Technologies			●			●
Software House						●
Video Insight			●			●
C = compatible with eligible integrated system						

### Proprietary Private Brand Hardware Common

Notice not all platforms use or are compatible with third party panels.

For example, major providers like Tyco's Software House use proprietary controllers, which differ and are not compatible with other Tyco access products like the distribution access line Kantech that uses its own proprietary panels.

Startups like [Openpath](#) and [Proxy](#) sell [3rd-party compatible mobile readers](#), but also are available in versions that use their own proprietary controller boards/relays in a standalone management software.

### Access ONVIF Not A Factor

When it comes to interoperability standards, access control is significantly less accepting of standards like ONVIF and no 3rd party standard is widely adopted.

As noted in [Access Control Does Not Want ONVIF](#), despite being so readily adopted by video platforms, both ONVIF interoperability standards, Profile A and Profile C have weak adoption with support from only two vendors:

ONVIF for Access Not Widely Used					IPVM
Product Name	Application Type	Profiles	Version	Date Approved	
AXIS A1001 Network Door Controller	Device	A C	1.65.2.1	2019-04-07	
AXIS A1801 Network Door Controller	Device	A C	1.84.1	2019-03-14	
TDSI Time and Data Systems International Limited					
Product Name	Application Type	Profiles	Version	Date Approved	
GARDIS	Device	A C	0.2.0	2017-11-26	

### Three Common Takeover Exceptions

While generally possible, 'takeovers', where controllers associated with one platform are switched to another, have exceptions.

The three common factors that complicate system takeovers and controller interoperability are:

- Unsupported Features/Integrations
- New Licensing/OEM Mask Codes
- Voided Warranty or Support

### **Unsupported Features/Integrations**

First, in terms of existing system integrations and features, just because another system supports the same controller hardware, there is no certainty a new platform supports the same range of features and integrations. Individual features, like OSDP or event cross-linking may be supported at the panel in one system, but not the other.

### **New Licensing/OEM Mask Codes**

Another pitfall, as noted in [Does Lenel Support Unbranded Mercury Security Hardware?](#) is some platforms may observe a 'Product OEM Mask' that codes hardware to a specific brand.

The codes are not always observed and not all 3rd party vendors have them in place, but adding existing hardware to a new system can be blocked and potentially require additional licensing fees or risk being refused by the new vendor.

In other cases, like Honeywell Prowatch, physically changing chips on the controller board may be required.

### **Voided Warranty or Support**

Finally, vendors may choose to not 'tech support' taken-over devices, nor do they typically warranty them when something goes wrong.

# OSDP

Access control readers and controllers need to communicate. While Wiegand has been the de facto standard for decades, [OSDP](#) aims to solve major problems of Wiegand.



In particular, OSDP's benefits:

- Bidirectional Communication, Including reader displayed feedback
- Standardized biometrics integration with access systems
- Handling large amounts Of credential data
- OSDP's 'Secure Channel' version supporting data encryption

However, the protocol has several significant issues impacting adoption, including:

- Unclear OSDP versions and profile definition
- Lack of OSDP conformance checking
- Vendors claiming only 'OSDP Support' is not enough
- No Official OSDP 'Conformant Products' directory

This report examines those issues and more basic details including:

- What OSDP Does
- Why OSDP Is Needed
- How OSDP is Organized
- What OSDP's Profiles Are
- Performance and Wiring differences between Wiegand and OSDP
- What 'Secure Channel' means for OSDP

## **What OSDP Does**

OSDP specifies communication protocol between readers and controllers, eliminating the need for 'proprietary drivers' when using 3rd party controllers and readers by simplifying how those devices communicate. Common functions are standardized, including how credential data is sent, formatted, and encrypted.

Advanced features such as which messages the reader displays, how integrated tamper or LEDs function, or even how bi-directional biometric verification works are also standardized. For the access market, OSDP's advantage is the specification can be used for 3rd party interoperability with many manufacturers.

## **Why OSDP Is Needed**

Access management vendors often do not design their own readers and controllers (and vice versa), and the necessary 3rd party interoperability has been handled by Wiegand for several decades.

However, OSDP improves or expands over Wiegand for maximum wire distance, total data transfer sizes, bidirectional communication, data encryption, and two-way biometric validation.

## **ODSP Key Elements**

The new protocol shores up those weaknesses and expands to offer:

- *Bi-Directional*: Allowing communication to travel both ways permits changes in real time, even allowing output behaviors like LEDs, Display Messages, or Sounder behavior to be changed dynamically. Depending on the reader, features like security keys or text fields can change based on the status of the system behind the reader.
- *Increased Throughput*: With OSDP, messages can be transmitted in stages, with each single message of 1,024 bytes, but layered in multiple messages. This means that far more than provisional 37 bit transfers are possible as someone presents a credential (fingerprint, face, or card) to a door.

## How OSDP Is Organized

Understanding OSDP versioning and profiles is complicated. In the past, OSDP versions have been released on a three-year interval, with versions released in 2011, 2014, and 2017. The current production version is 2.1.7, from 2017.

The complete versions of OSDP include more criteria and features than single products include, so SIA maintains several different 'OSDP profiles' applying partial implementations based on type of product. These profiles include:

- [Basic](#): This profile is the one most typical card and fob access card readers will support at a minimum
- [Biometrics](#): This profile addresses '2-way verification' for biometric readers, exchanging templates with central access systems.
- [Extended Packet Mode](#): For device designed to interact with smart card layers or advanced security standards [like FICAM](#), or mobile credentials, this profile describes standardized formats for large or complex data.
- [Peripheral](#): For 'minimal' devices that do not include reader output display, biometrics support, or 'large' multi-part message support.

## Generic OSDP Support Claims

Despite vendors claiming 'OSDP compatibility', that alone is not enough to assess which versions, profiles, or features are supported. Neither SIA, nor member companies, make this clear.

For example, [this HID iClass SE reader only claims' OSDP' support](#) but does not explain which version or profiles are supported:



### HIGHLY ADAPTABLE AND SECURE HIGH FREQUENCY ACCESS CONTROL SOLUTION

- **Powerfully Secure** - Provides layered security beyond the card media for added protection to identity data using SIOs.
- **Adaptable** - Interoperable with a growing range of technologies and form factors including mobile devices utilizing Seos®.
- **Interoperable** - Open Supervised Device Protocol (OSDP) for secure, bidirectional communication.
- **Versatile** - Extended range is available for applications such as parking and gate control solutions.



No Version or Profiles Given

The lack of clarity regarding what types/versions of OSDP vendors support, and when asked about this, SIA assigned responsibility to buyers to make this clear:

For now **access control buyers need to communicate with their vendors** on the OSDP profiles that they support, Basic, Secure Channel, Biometric, etc. While this system of communication and trust was not too much of an issue when only a few vendors were offering OSDP solutions we realize that this model will not work for long, and as stated, we will be working to address this.

This answer illustrates the significant clarity issues buyers face when specifying OSDP.

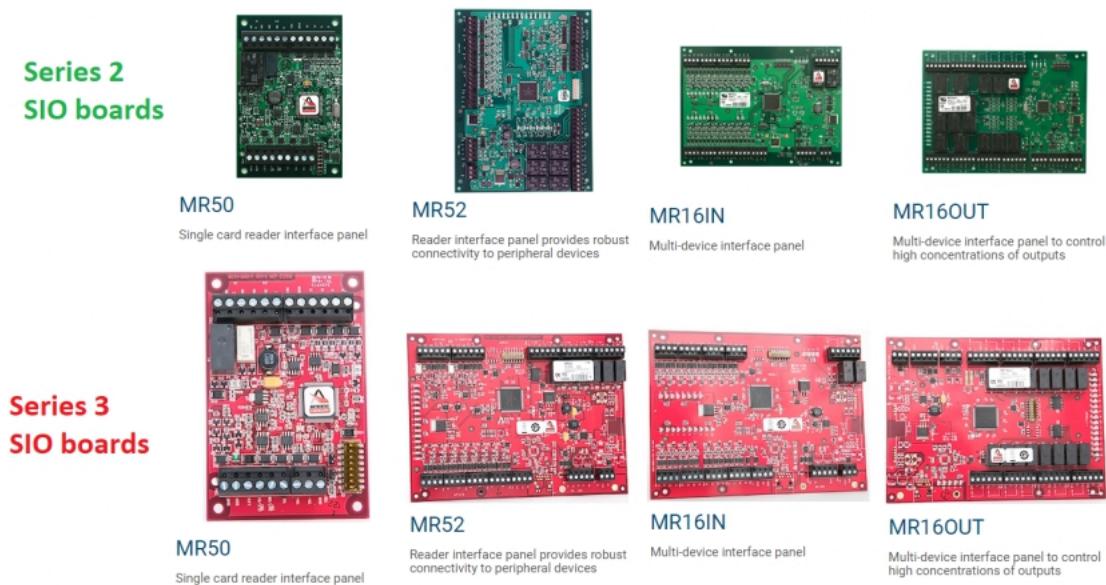
## Limits Of Upgrading OSDP

As updated versions or profiles are released, the ability to upgrade existing hardware in the field is not always possible.

In general, if hardware designs include sufficient physical resources and ability to update embedded firmware, a simple upgrade can be done to installed equipment.

However, access readers and control panels are often 'computing constrained' devices that cannot support these updates or increased functionality and they must be physically replaced.

A common example of this is found in Mercury Security panels, with the older 'Series 2' SIO boards versus 'Series 3 Redboards'.



One of the biggest factors in the development of 'Series 3' hardware was additional processing onboard to support OSDP encryption released with version 2.1.7 'Secure Channel', while other devices like [Axis A1001 controller](#) was accomplished with a firmware update.

### Comparing OSDP vs. Wiegand

The prime features of both are compared in this chart:

Wiegand vs. OSDP		IPVM
	Wiegand	OSDP
Distance	~150 m	~500+ m
Bidirectional Comms	No	Yes
Encryption	No	128-bit AES for Secure Channel Versions
Tamper	Optional	Included
Cabling	Typically Copper	UTP, Serial, TCP/IP
Biometrics Support	Unidirectional	Bidirectional

## OSDP Weaknesses

However, OSDP presents several new problems including:

- *More Complex Wiring:* Unlike Wiegand, using OSDP requires non-standard reader terminals and wire jacket colors and may require additional electrical resistors installed in the panel, potentially driving installer complexity and adding extra labor.
- *Multiple Profiles:* As mentioned above, no single OSDP profile is comprehensive and more than one OSDP profile is needed, complexity not needed when using Wiegand. (See 'Multiple OSDP Profiles' above for more detail.)
- *Self-Policing Conformance:* SIA offers no claim conformance checking, and similar to [List Of Manufacturers Faking ONVIF Conformance](#), the risk of manufacturers faking OSDP conformance is a fundamental risk and causes uncertainty.

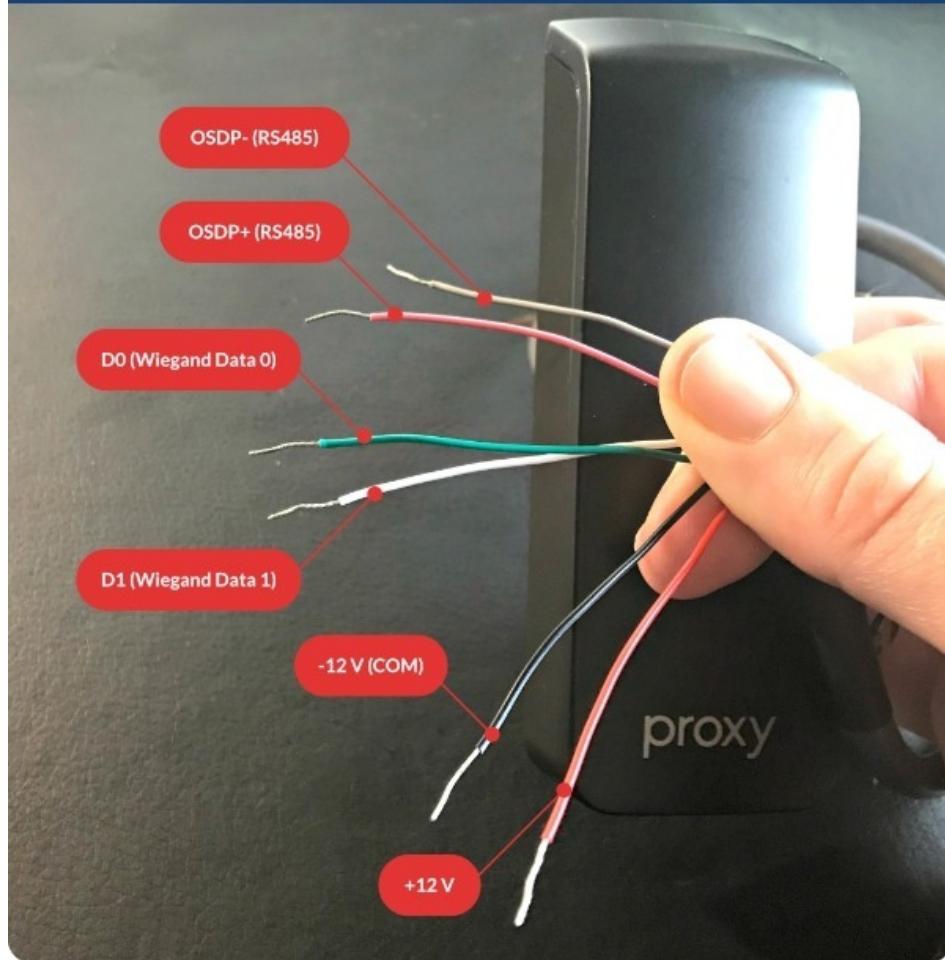
## OSDP Wiring Uses Different Terminals & Wires

Many readers support both Wiegand and OSDP, but require using distinct conductors for either type.

The image below shows an example reader supporting both protocols with separate wires to connect depending on type:

## OSDP Uses Alternate Reader Wires

IPVM



OSDP requires only two conductors for data and two for power, while Wiegand requires far more for individual reader functions.

Wiegand's extra conductors result in substantially large pigtails with bundles of ten wires or more. If OSDP readers have large pigtails, it is due to offering either Wiegand or OSDP connections as an option.

The terminal connections for this [HID iClass SE reader](#) illustrate nearly 14 wires are included in a pigtail. For this reader, the 'red/green' wire (P2-7 terminal) and 'tan' (P2-6) connectors are dedicated for OSDP:

PIGTAIL***	TERMINAL	DESCRIPTION
Yellow	P1-1	Beeper Input
Orange	P1-2	LED Input (GRN)
Black	P1-3	Ground (RTN)
Red	P1-4	+VDC
Drain	P1-5	Unused
Brown	P1-6	LED Input (RED)
Blue	P1-7	Hold Input
Red/Green	P2-7	GPIO1/OSDP (RS485-FDX/HDX-A)
Tan	P2-6	GPIO2/OSDP (RS485-FDX-HDX-B)
Violet	P2-5	*Open Collector Output/Tamper
White	P2-4	**Wiegand Data 1 / Clock
Green	P2-3	**Wiegand Data 0 / Data
Pink	P2-2	GPIO3 (RS485-FDX-Z)
Gray	P2-1	GPIO4 (RS485-FDX-Y)

Unlike Wiegand, where 'white' and 'green' are typically standardized colors, OSDP wire colors are not, which can lead to installer confusion.

### Not a 125 kHz or 13.56 MHz Format Issue

OSDP does nothing to mitigate or improve the fully cracked vulnerability risk of using 125 kHz formats, like the one detailed in [Hack Your Access Control With This \\$30 HID 125kHz Card Copier](#),

Indeed, even if 'secure' [uncracked DESFire or iClass](#) cards are used, if the reader communicates with upstream controllers using an unencrypted protocol like Wiegand the system is vulnerable to attacks that intercept and rebroadcast card reads.

## 'Secure Channel' Encryption

Starting with [OSDP version 2.1.7](#) uses 128-bit AES encryption on data between reader and controller. Previous versions of OSDP may not support encryption, as it was not defined 'mandatory' until then.

With OSDP Secure Channel, the protocol between reader and upstream controller is encrypted against easy interception and potential copying with 'man in the middle' devices. For example, [the BLEKey](#), installation takes about 60 seconds, can be done from the public/unsecured side of the door, and is undetectable by the system and system managers.



Almost every access system is vulnerable to the risk of Wiegand copying when skimmers are installed in the reader. The card information they intercept can then be used to create identical copies of valid cards or to inject valid Wiegand signals in systems bypassing readers entirely.

The video below shows how these skimmers are typically installed:

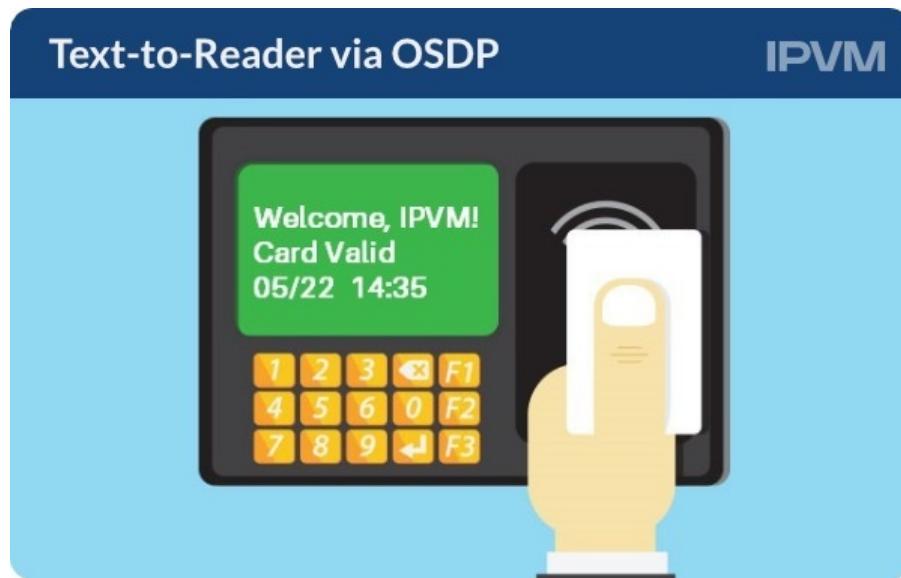
[Click here to view the BLEKey Install video on IPVM](#)

Wiegand sniffers are easy and inexpensive to get, with kits typically [running ~\\$35 - \\$50 online](#).

### Reader Displayed System Messages

One OSDP feature not possible via Wiegand is the ability to push system information and user prompts to readers.

This allows for preemptive messages to be displayed to new users, contact numbers for visitor access, and information like dates and times to be shown for time clock applications:



Of note, the 'Peripheral' OSDP standard does not support this feature and is only available in the 'Basic' and 'Biometric' versions.

### Biometrics Support

An interesting aspect of OSDP is how biometric authentication is supported using the bidirectional data passage between system and reader.

Typical Wiegand biometrics perform biometric template comparisons within the reader in databases stored in the reader or other potentially risky application, but using OSDP offloads

template storage to access systems that push them down to readers only when queued on demand.

The image below shows how the exchange typically works:



The 2-way data exchange allows for potentially faster verifications, criteria that IPVM will incorporate in a future round of OSDP Biometrics test.

## Reader And Controller Support Required

An aspect of using OSDP that is not well understood: both reader and controller must support the protocol.

Unlike Wiegand, the default protocol that often requires no additional configuration during install, OSDP typically requires setting the controller, as the image below shows:

The screenshot shows a software interface for configuring readers connected to a controller. At the top, it says "OSDP Requires Controller & Reader Support" and "IPVM". Below that is the "AXIS COMMUNICATIONS" logo. The menu bar includes "Overview", "Access Management", "Alarm Log", "Event Log", "Reports", and "Setup". The "Setup / Hardware Configuration" page is active. A large box titled "Configure readers connected to this controller" contains settings for "Entrance reader" and "Exit reader". For the "Entrance reader", the "Protocol" is set to "OSDP, RS485 half duplex" and the "Connection" is "Active low". A red callout box with the text "OSDP Requires Controller Configuration" points to the "Protocol" dropdown. For the "Exit reader", the "Protocol" is set to "Wiegand" and the "Connection" is "Active low". At the bottom right are "Cancel" and "Finish" buttons.

**OSDP Requires Controller & Reader Support** **IPVM**

AXIS COMMUNICATIONS

Overview Access Management Alarm Log Event Log Reports Setup

**Setup / Hardware Configuration**

**Configure readers connected to this controller**

Entrance reader      Entrance reader protocol:  
  Wiegand      Single LED ▾  
  OSDP, RS485 half duplex

Entrance REX      Entrance REX connection:  
  Active low ▾  
  REX does not unlock door

Exit reader      Exit reader protocol:  
  Wiegand      Single LED ▾  
  OSDP, RS485 half duplex

Exit REX      REX connection:  
  Active low ▾  
  REX does not unlock door

Cancel Finish

There are examples of 'auto detection' for OSDP in some products, [like Wavelyn Ethos readers](#), but automatic configuration is not part of the default OSDP specification.

### **Controller Resistors Sometime Required**

Of note, some controllers call for the use of resistors on OSDP readers, especially on long cable/daisy chained reader runs or where EMI may be a concern:

**Note:** For OSDP cable lengths greater than 200ft. (61M) or EMI interference, install  $120\Omega \pm 2\Omega$  resistor across RS-485 termination ends.

While 'end-of-line' resistors are not uncommon with intrusion alarms, requiring them for reader use in access is not typical with Wiegand and may be an unexpected, albeit trivial, additional cost.

### **Self-Policing Conformance**

Compounding the risk of false claims is that SIA does not check or oversee products claiming OSDP conformance, and no external group is tasked to do so.

SIA commented:

'There is no 3rd party that verifies claims of OSDP compliance. The OSDP Working Group (WG) started off as a small group of vendors working on improving and adding to the legacy OSDP including tools for them to verify that they are doing OSDP correctly.'

Now that we've seen a spike in the number of vendors participating in the OSDP WG and also claiming support we realize the need for a verification/certification program and are working on that process now.'

SIA [offers a conformance testing tool](#) but the utility is not a simple GUI, requiring some development or technical skill to use.

## No OSDP Conformance List

Another complication is there is no centrally managed list showing which devices are conformant and which are making untested claims.

Unlike [ONVIF, who publishes a list of 'conforming' devices](#) per the Profile they claim, OSDP does not offer or track in a similar way.

## OSDP Support Growing, but Still Limited

Vendors claiming OSDP support are mostly mainstream commercial access brands including HID Global/Mercury Security, Wavelyn, Axis, Software House, Lenel, Suprema, Farpointe Data, Rosslyn, and Cypress.

In terms of vendors not supporting OSDP, 'Hospitality' brands, Hikvision, and many distribution access lines like ProData Key do not.

SIA tells IPVM the number of vendors producing OSDP equipment is 'around 40-50, the majority being peripheral device (reader) vendors'.

However, unless the incomplete or uncertain conformance aspects of profile support are better defined, the effort may face adoption problems and subsequent rejection for the more trusted Wiegand standard.

# Access Control Management Software

In access control, the locks, readers and credentials may be what most see but its the management software where everything is controlled. We cover the most common parts of this software and provide an overview of how the pieces relate to managing an access system.

## Basic Purpose

The function of Access Control Management software is fourfold, with distinct functions and management focuses:

1. *Live View*: Displaying the current state of the access system; if doors are locked/unlocked, and which users are interacting with doors.
2. *Door Management*: Configuring every opening is critical, to ensure it opens and remains locked on schedule or depending on credential.
3. *Cardholder Management*: Administering all potential users for their needed access privileges, and updating those records as needed.
4. *Reporting*: This offers users to forensically review log details collected by the system - when and where credentials were used, and when openings were unlocked.

We examine each of these four areas inside.

## Essential Elements

While each management platform varies based on appearance and terminology, it contains the same basic elements. These include:

- Monitoring Interface

- Configuring Doors & Controllers
- Access Rule Creation and Application
- User/Credential Management
- Access Schedule Configuration
- Report Creator

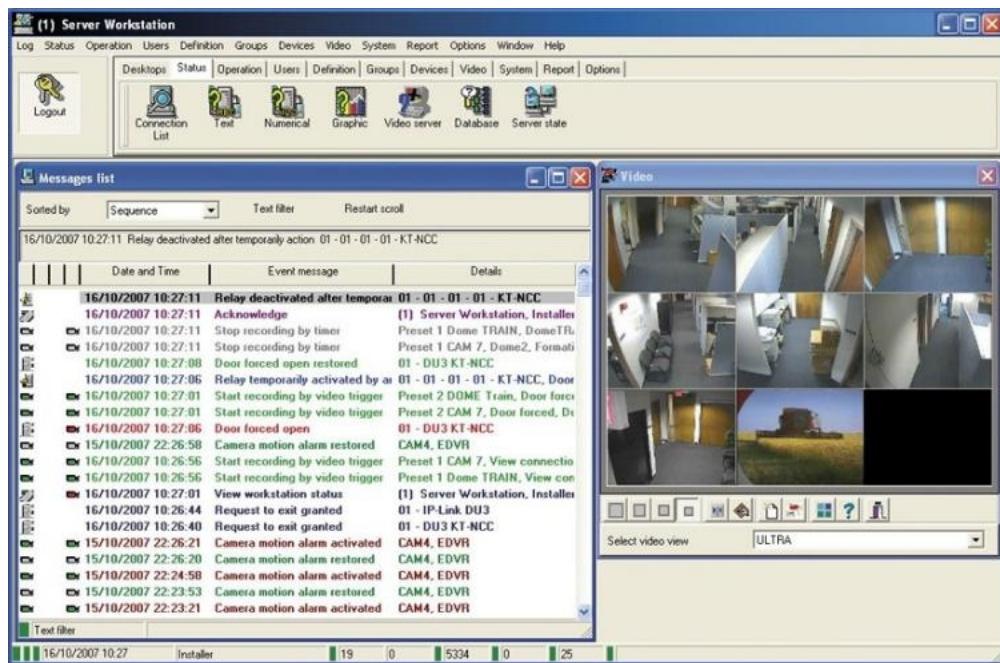
In many cases, these elements are contained in a server or appliance separate from door controllers. System designed for smaller numbers of readers and doors may be hosted on a dedicated panel, but enterprise systems may require several servers to host the features and integrations of large numbers of doors.

### **Monitoring Interface**

Live View allows operators to peer in to the current state of doors in real time. Exact interface features and layout vary, but most include:

- *Door Events*: Every time someone requests passage through a door, a lock released, or a door is opened the event is logged.
- *Alarm Report*: If someone holds a door open too long, forces a door open, or attempts using an invalid credential, the interface sends an alert or draws operator attention to the event.
- *Lock/Unlock Controls*: An operator has the option to manually unlock or lock a door remotely, often to all doors in a single 'lockdown' operation.

This screenshot shows how this information is typically displayed and organized, usually in a timeline of event messages:



The video below gives an overview of this element:

[Click here to view the Access Management Software – Live View video on IPVM](#)

Video Integration usually displays live video feeds next to badge photos so operators can visually verify the person entering is valid:



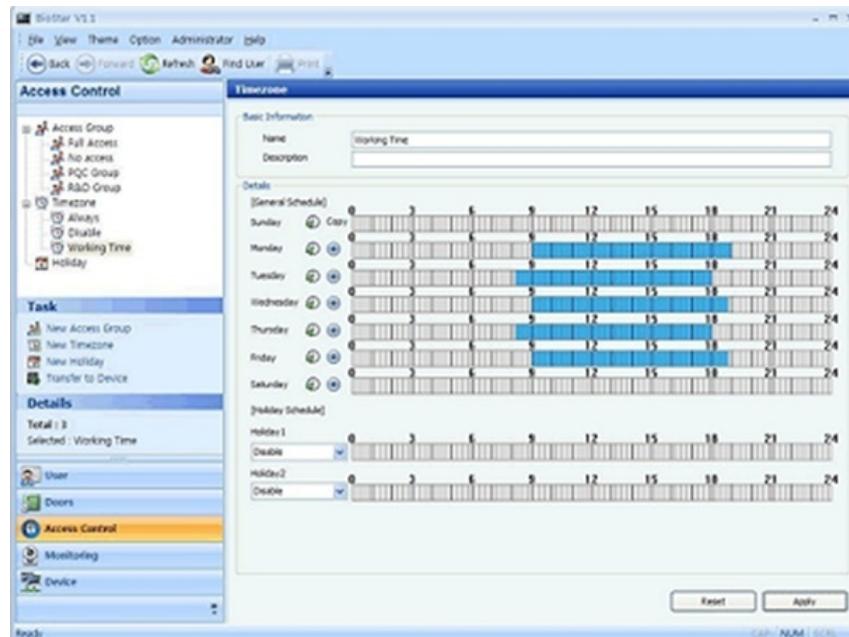
## Configuring Doors and Controllers

The management platform provides the ability to add new controllers and to tweak configuration of those devices to fit each opening. Because each opening is used differently, even doors consisting of the same hardware may need to be slightly altered for efficient use. The videos below shows the 'typical' features to expect when doing these actions:

[Click here to view the Access Management Software – Adding Doors & Controller video on IPVM](#)

## Access Rules and Schedules

The key advantage of electronic access control versus mechanical locks and door keys is the ability to restrict when and when credentials can be used. Some platforms enforce these rules against doors, while others associate them with specific cardholders. Schedules and levels are commonly configurable down to exact seconds:



Other platforms combine either option, granting a group of physical doors or cardholders enhanced security privileges. The videos below show off the basics of these features:

## *Access Rules*

[Click here to view the Access Management Software – Access Rules video on IPVM](#)

## *Access Schedules*

[Click here to view the Access Management Software – Schedules video on IPVM](#)

## **User Management**

Access management extends beyond just configuring doors. Every user, and the credentials they possess, are integral pieces of any system. The common user management functions headend software include:

- Adding or Changing Users
- Associating Credentials with Users
- Printing Badges

The videos below provides an overview of these features:

### *Adding Cardholders*

[Click here to view the Card Holder Management video on IPVM](#)

### *Adding Credentials*

[Click here to view the Building Credentials video on IPVM](#)

## **System Reports**

A key feature of management, querying activity logs is the equivalent to searching for recorded video. The clip below is a short overview of what to expect and how it is organized in an Access Management software:

[Click here to view the Reporting video on IPVM](#)

# Securing Access Control Installations

The physical security of access control components is critical to ensuring that a facility is truly secure. Otherwise, the entire system can be circumvented or shut down by an adversary.



In most cases, if done correctly, adding layers of security and protecting access components adds negligible cost. Here are IPVM's 5 recommended steps and options:

- Install Controllers on Secure Side of Openings
- Keep Panel Closets & Server Rooms Locked
- Lock Enclosures & Panels
- Use Tamper Sensors & Alarms
- Integrate Surveillance Cameras

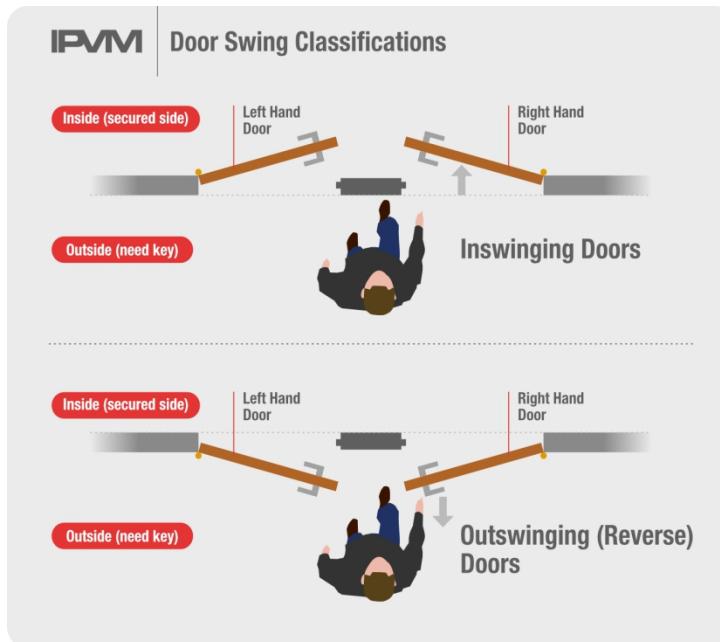
Finally, the quiz at the end will test your knowledge.

## Install Controllers on Secure Side of Openings

The 'access controlled' side of the opening is typically the inside area unless dealing with prisons or other applications where one is trying to lock people in.

When a door is access controlled, the intent is to keep those unapproved to enter on the 'unsecured side' so occupants are safe, also called the 'secured' side. While the exact usage of these terms differs, most characterize the 'inside the locked door' to be the secured area.

The image from our [Door Swing Primer](#) illustrates the difference in Secure vs Outside side of doors:



Locating sensitive control equipment on the unsecured side leaves it a target to those attempting to force entry.

Because the unsecured side is not controlled, steps should be taken to mitigate the risk of exploiting or breaking access control devices. A fundamental step is to install as much of the access control hardware (controllers, power supplies, cabling) on the safe or secured side.

While this may seem to be a bit of common sense, it is commonly overlooked. Take this example:



This image shows the 'unsecured' side of the door, with the keypad reader and mortise lock facing outside the locked door. However, the technician has mounted the critical door controller in plain sight above the opening on the locked side.

However, risking exploits and tampering is easily mitigated by mounting access hardware on the secured side of the opening. Typically the decision is the same cost and puts expensive and potentially vulnerable devices in a safer area.

Even after being located on the secured side, mounting hardware in a discrete location is prudent. Simply locating devices at the door above the opening above ceiling tiles puts access control literally out of reach, out of sight, and out of mind for potential threats:



When it comes to access control, the risk of any exposed power/control cabling should be avoided during design.

More than just controllers or interface modules are at risk. Take the example image below, of a maglock securing an outside entrance door:



In order to defeat the maglock entirely, only the exposed cable needs to be cut. We note the proper remedy to the issue above in our [Maglock Selection Guide](#), where in-swinging door maglocks need an armature bracket.

#### Keep Panel Closets & Server Rooms Locked

Traditional access control systems use central panel or servers to coordinate activity, and even 'edge' types of systems typically use centralized network closets.

IT or Building Security policy generally dictates these locations be kept locked and access to select few, so naturally, these doors are commonly controlled by the same access system they are protecting:

## Deploy Access Controlled Server Racks IPVM



For these areas, and server racks, using PINpads or keypads is insufficient, despite being common. PINs and codes can be shared, and commonly are, over time leaving these areas uncontrolled or very loosely regulated.

Moreover, setting appropriate [Access Control Levels and Schedules](#) for Panel Closets & Server Rooms keeps unauthorized employees from entering sensitive areas like server rooms if they could present a risk.

While most users do not challenge the cost of adding main control closets to the facility access control system, consider that even 'minor' closets should be locked as well. When the cost or need of adding access control is hard to justify, a well-managed system of mechanical locks and keys, or even a 'stand-alone' electronic lock keeps the risk at bay.

### Lock the Panels & Enclosures

Even when kept within locked closets, those areas often are shared with other types of mechanical systems like plumbing, telecom, or even janitorial staff. While components or panels may be locked away for the general public, there may still be the risk of unauthorized individuals tampering with systems.

Most enterprise access systems include lockable enclosures, like the ones shown below:



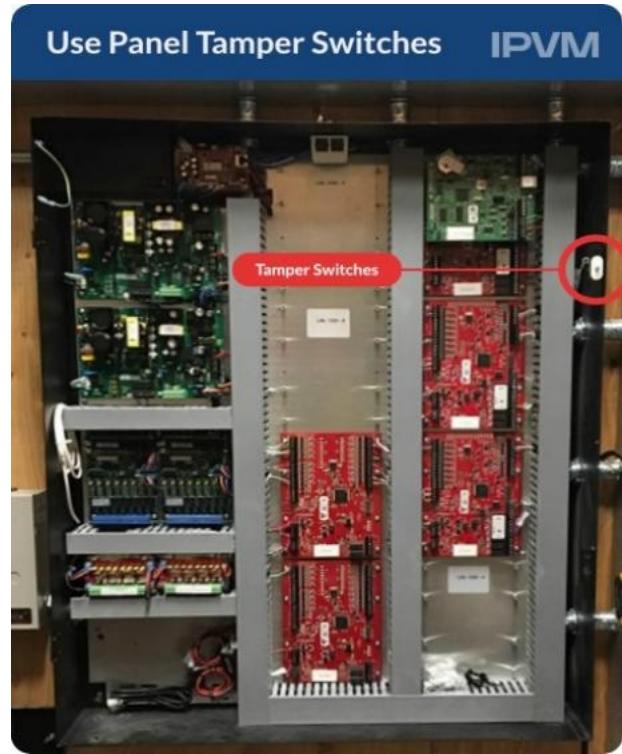
Every enclosure 'can' includes a cover that is kept locked at all times. This extra step ensures that spontaneous tampering is avoided, and simply keeping controllers locked down and tightly managing the keys is a prudent, low-cost step.

### Use Tamper Sensors & Alarms

Many devices and panels include a 'tamper switch' that essentially detects when a device has been knocked off a mounting point or a panel has been opened. Unfortunately, these switches are often left uninstalled or unconfigured to send alarms, since they do not represent a core feature of the system.

However, considering how quickly locks can be jimmied or controllers knocked off the wall, seconds count. Properly configured tamper switches can notify authorities in seconds when tampering occurs, rather than being discovered hours after the fact.

Most systems include hardware tamper sensors or switches, and configuring them for use takes minutes - another inexpensive, but valuable method of monitoring system integrity:



### Integrate Surveillance Cameras

Finally, perhaps the most expensive option can also provide visible deterrence and immediate feedback: integrating video and access together. When cameras are located near access-controlled openings, potential tampering or unauthorized entry attempts are caught on camera.

Especially when the facility's surveillance system is actively monitored, quick response can stop damage or intrusion before it occurs.

However, while very effective, the cost of integrating the two systems together can be moderately expensive (several hundred dollars per door) and require additional cameras if not already installed. In most cases, the integration between the two systems will be used for more than just occasional detection of threats, but typically for the verification of those passing through the doors:



## Use OSDP

While not a physical security consideration like locking enclosures or tamper switches, OSDP monitors the reader bus by supervising the connection between the controller and credential reader.

Unlike Wiegand, which is unidirectional and pushes data from reader to controller only, OSDP is bidirectional and can alert system users if someone physically separates the device from the system.

For more on OSDP, catch our [OSDP Access Control Guide](#).

## Quiz Yourself

Take the [Securing Access Control quiz](#) now.

## Access Control Records Maintenance

Weeding out old entries, turning off unused credentials, and updating who carries which credentials is as important as to maintaining security as keeping equipment operational.



Failing to do so can be as dangerous as leaving a door wide open. Unfortunately, this often gets overlooked as busy work and sometimes to disastrous consequences.

We examine:

- Best practices for Cardholder Management
- How to Maintain Records and System Databases
- Benefits of Proactive Maintenance
- Do Not Reuse Credentials

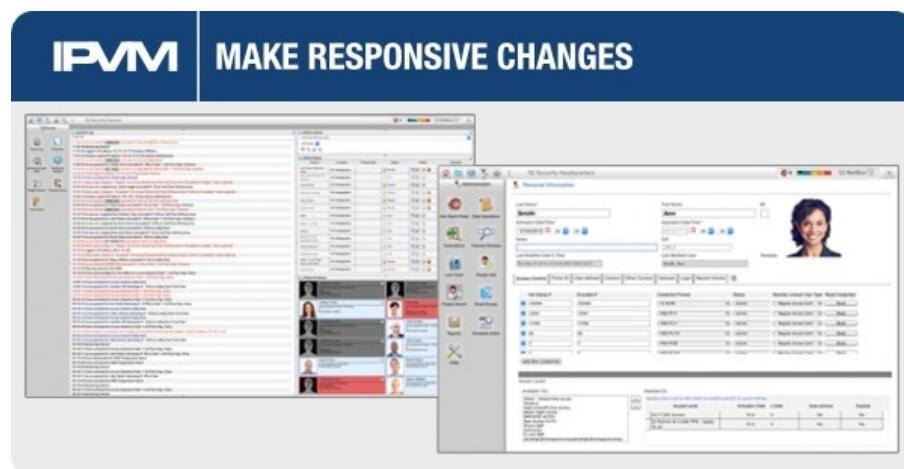
### Best practices for Cardholder Management

Steps needed to keep the database trim and current are not difficult but their importance can not be understated:

- *Involve Human Resources:* With Electronic Access Control, a formal line of communication between HR and Security must exist. As soon as employment status

changes (ie: terminations, relocation, promotions) feedback needs to be channeled to those responsible for access control. Just as IT Departments terminate/change network access or emails, Security must respond accordingly with Access Control changes.

- *Formal Reporting Out:* Similar communication initiated by Security groups should notify HR, Department Heads, and perhaps even employees / their direct supervisors when any configuration change to credentials occur. This helps close the loop of communication, but also reaffirms the importance to all why communicating these changes to Security is important.
- *Collect & Invalidate Credentials:* Aside from just software configuration changes, write policy to include physically taking possession of credentials during an employee termination or transfer situation. Even if the credential cannot be reissued, ensuring it is properly disposed of will mitigate the potential for misuse.
- *Make Responsive Changes:* Finally, do not delay in making configuration changes to the card holder database. Even if seemingly inconsequential (ie: inter-department transfer, shift change, name change) the opportunity to keep records up to date may be lost or create operational issues if delayed. Many times, managers do not consider the impact of employee changes on subsystems like Access Control, acting immediately on changes can reveal operational questions that can be asked before becoming an issue.



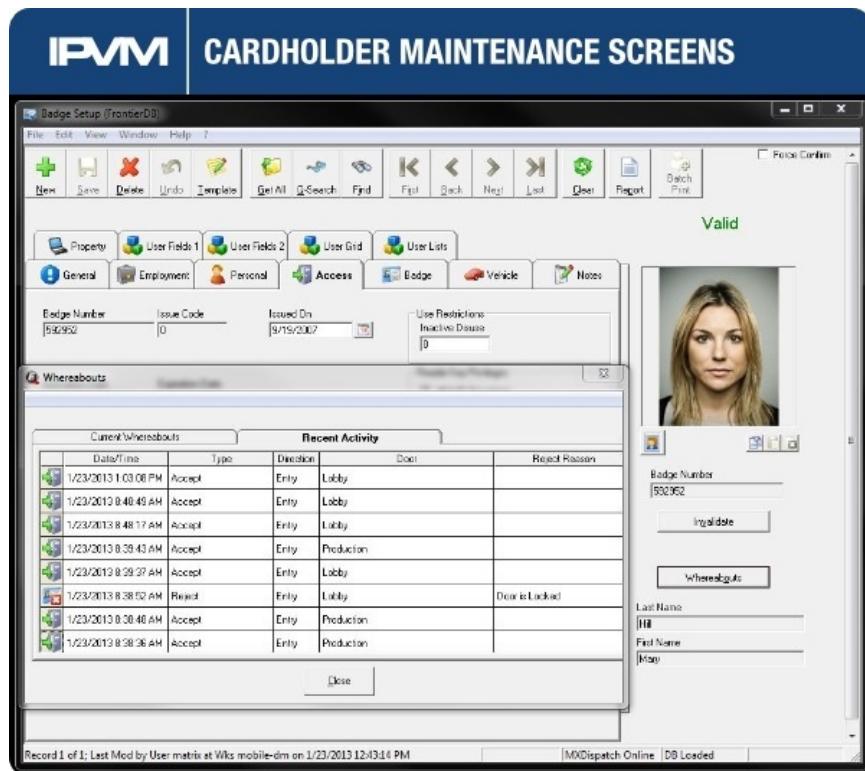
## Do Not Relegate Upkeep As 'Busy Work'

The most critical management step for access records upkeep is to make it an operational priority, not an afterthought.

As central as this database is to access control, keeping it current is often considered 'paperwork' to be performed by clerks or by staff when less critical work slows down. While the nature of this upkeep is not complex, it is a mistake to consider it 'busy work', as not keeping it up to date can have negative security consequences.

## Access Cardholder Maintenance

While specific screens vary, all access control systems include a management tool to administer user information, similar to the image below:



During normal operation, this management screen is not often used, and once a credential is provisioned it may not be looked at again. However, knowing the value of the data it contains should not be underestimated.

## Automated Database Maintenance Tools

Most databases include a light maintenance application that should be periodically run to 'tidy up' data tables and repair broken elements before causing access failures. For example, the [Microsoft SQL Server Agent](#) performs the following tasks:

1. Reorganize/rebuild scatter index or data tables
2. Shrink data and log files by removing empty entries
3. Backup database and transaction log
4. Perform internal consistency checks

Maintenance applications often also perform Date/Time Syncs between applications and edge controller devices, so that congruity in logging is kept.

## Access Database Maintenance Matters

The benefit of keeping records current range from Life/Safety benefits, to keeping IT systems responsive:

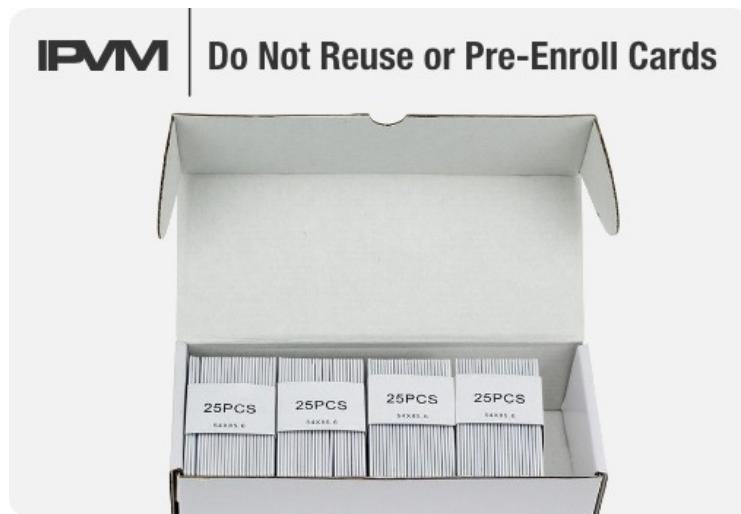
- *Quicker Operational Response:* Understanding the actual effect of a 'lock down' situation relies on assuming the user database has impacted all potential card holders. For example, when using [Access Control for mustering](#), each identity listed in the database must be accurate. Non-maintained databases will not be useful for that application, simply due to neglect.
- *Better Performance:* From a functional standpoint, bloated databases increase the potential of error and time needed to process through them. The inefficiency built into operation from unkempt databases can range between increase 'wait' times to read a card, to undetected corruption/[unauthorized duplication](#) of card holder records.

- *Needs Change Over Time:* Even if a feature or piece of data is not currently 'used' to identify users or grant access, remember that system use parameters change over time, and once a database is 'ruined' with bad or lost information, it is costly to recover. In many cases, keeping fields accurate and updated can provide a critical, defining key to handling card holder data that may result in a costly manual effort otherwise.

### **Do Not Reuse Credentials**

Not all end users choose to personalize credentials as ID Badges, and as a cost-saving step repeatedly reissue credentials. Once cards are turned in, they are thrown into a drawer until they are again issued. In this situation, turning in a card is not enough, the credential must also be removed from the system.

It is also common to destroy or dispose of the credential at this stage too, to mitigate the risk of illicit use or uncontrolled examples to circulate for 'reverse engineering' in potential duplication.



If user accounts are not kept current, a credential may be handed out with the previous identity. Uncovering these discrepancies can be time-consuming and frustratingly costly.

## **Another Name for "Key Control"**

Keeping this data up to date is another form of managing keys, called 'key control' by many. Auditing which keys are currently in circulation, who carries them, and which doors they can open is a critical part of determining where gaps in security exist. For more details on this, see [Key Control For Access Control Tutorial](#).



In similar fashion, pulling a usage report quarterly or twice yearly to see which cards have been used, and which ones have not, will help identify old credentials that should be turned off or help uncover those who might be using a mechanical key to gain access instead of their authorized credential.

[Note: This guide was originally written in 2013 but substantially revised in 2019.]

# Networks and Cable

# Cabling

Access Control is only as reliable as its cables. While this aspect lacks the sexiness of other components, it remains a vital part of every system.



We look at the types of cables used by these systems, including 22/4, 18/6, 22/2, and where special attention should be spent when installing them.

## Defining the Cabling Needed

Access control systems use three methods to carry data between components:

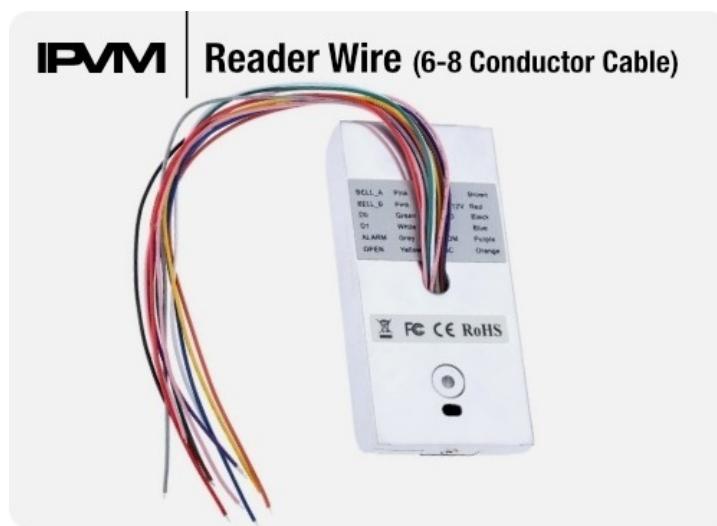
- Ethernet, or IP-based Systems
- Hardwired Serial-connected Systems
- Wireless Systems

Even wireless systems generally use some cabling, as the components on the door (eg: readers or door position switches) often are hardwired even if the controller is not.

Most systems specifically define which type of cabling to use, depending on which device is being installed. We examine the three most common wire types, and where they are used in access, below:

## Reader Wire (6-8 Conductor Cable)

Typically used to connect Readers to Controllers, this bundle of connectors breaks down to where each conductor color handles a unique function of the reader. However, 'extra' functions (like reader beeper, or reader LEDs) may call for additional conductors, and items like power and drain wire are included apart from conductor count. The chart below details a wiring schematic for a [proximity-style mullion reader](#):



Schematically reader wire color generally indicates the function of individual wires. For example, power is often red & black, data is typically green & white, and other features like beep, tamper, or LED color are reserved for other strands.

Here's one example of these assignments or instructions for wiring readers:

Wiegand	Clock & Data	Wire Color
+DC	+DC	Red
Ground	Ground	Black
--	Card Present	Violet
Data0	Data	Green
Data1	Clock	White
Shield Ground	Shield Ground	Drain
Green LED	Green LED	Orange
Red LED	Red LED	Brown
Beeper	Beeper	Yellow
Hold	Hold	Blue

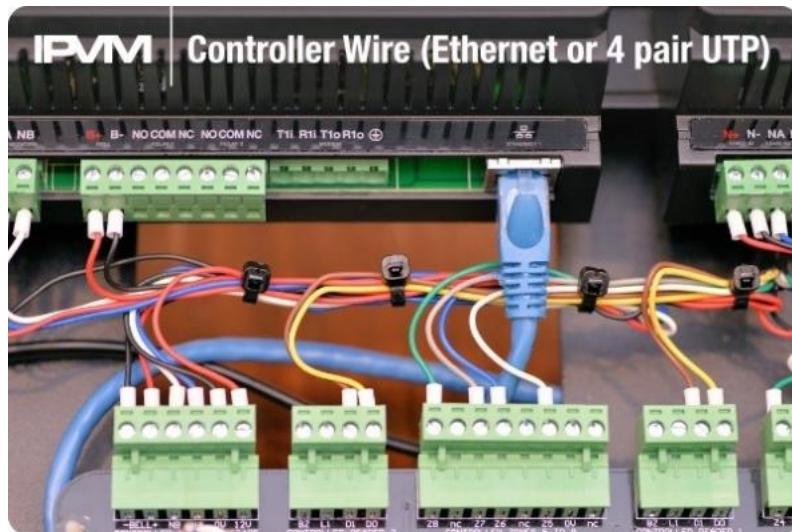
### Controller Wire (Ethernet or 4 pair UTP)

This cable is commonly used between the main control panel and door controller, and may cover long distances as a result. Door devices like [PIR 'Request to Exit' devices](#) or [door operator controls](#) are wired using this type.

Unlike ethernet cabling standards that limit runs to 100 meters, these connections can span thousands of feet using the same type of cable. In most cases, while a range of cabling options will work, it is still best practice to employ whichever type the manufacturer recommends, as tech support and product warranties often depend on installing to specification:

Connection	Maximum Distance Communication (ft)	Cable Requirement
bright blue to SBB-RI	4000	18 AWG/2 Pair, Strd, Twst, Shld
SBB-NRI to Power Supply	N/A	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to AD-300	4000	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to Schlage VIP At 12 Volts DC	4000	18 AWG/2 Pair, Strd, Twst, Shld
At 24 Volts DC	4000	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to PIM400-485-SBB	4000	18 AWG/2 Pair, Strd, Twst, Shld
bright blue to PIM-SBB	1000	18 AWG/2 Pair, Strd, Twst, Shld

Here's an example of an ethernet connected controller and how the RJ-45 jack is typically located with other wiring types:



### Lock & DPS Wire (1 Pair)

This cable is typically used to deliver power to devices, like maglocks, strikes, or other accessory devices like illuminated RTE Push Buttons. It may also be used to wire contact sensors, door position sensors, and to cameras for I/O linked functions.

These wired connections are often just a black and red pair in a service tail from a device, like this maglock below:



## Drain/Shielding Wires

Many door control devices are equipped with 'drain' wires that are included for use when a door exists in a 'noisy' RF/EMI environment. The extra wire acts as a grounded sink for ambient interference around the bundle, and helps maintain transmission between reader/controller or controller/panel.



For more, read our [Drain Wire For Access Control Reader Tutorial](#).

## Which Gauge to Use?

Wire gauge, or thickness, is a key aspect determined by cable run distance, voltage and amperage draw. The manufacturer specifies the wire's specific gauge. The most common gauges chosen in access control are 24, 22, 18, and 16 AWG sizes. In general, greater voltages and longer distances call for larger diameter wire (lower AWG number). Each component may specify different wiring, and the cable specification may change according to total distance / type of voltage used.

## Combining Cables

Unlike IP cameras where a single cable typically connects a device, an access controlled door require several different types of cables. For example, there might be a 6 conductor bundled with 4 and a 2. Here are a few examples of common combinations:

- 18/2: Lock Power
- 18/6: Reader Power/Communication
- 22/4: RTE Buttons/PIR
- 24/2: Door/Latch Position Contacts

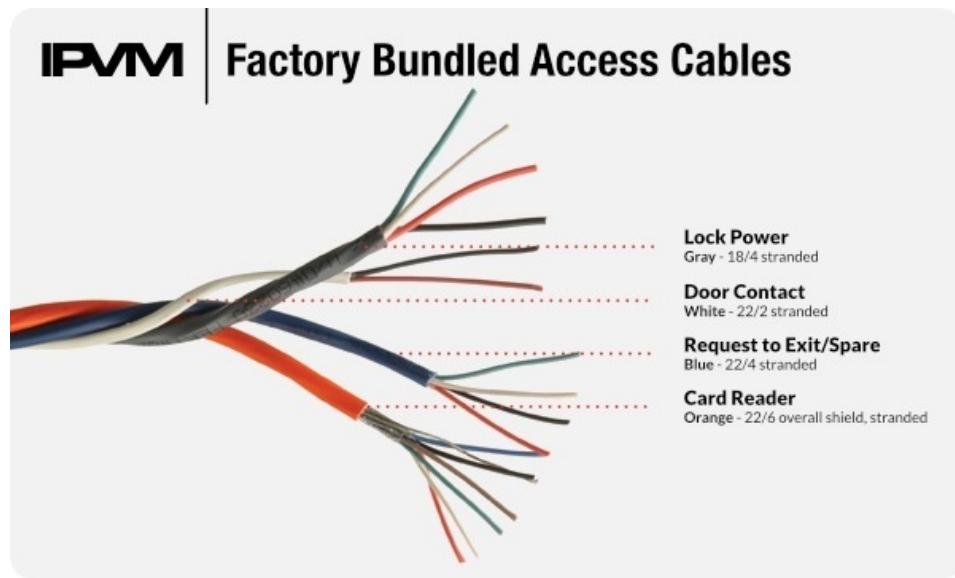


The specific configuration of cables depends on the mix of devices used at the door. However, the number of cables normally will not exceed 4 or 5 types, and in some cases multiple devices like contrats and RTE devices can be connected on the same pair.

## Factory Bundles vs DIY

These combinations may be delivered as a factory bundle or combined by the installer locally.

Many cabling suppliers offer factory bundled cables composed of the common conductors and kitted at the factory wrapped together or sealed into a single jacket. The image below is an example of a bundled product and the types of cable it contains:



*Bundle Pricing:* While many configurations of bundle cables are available, they typically cost more per unit length than separate cables pieced together manually. Take the example below:

- 1,000 feet of Factory Bundled Cable @ ~\$1,250 or about \$1.25 per foot.

*Discrete Pricing:* Compare that to 500 feet quantities of individually pieced cables:

- 18/4 @ \$125
- 22/2 @ \$50
- 22/4 @ \$75
- 18/6 @ \$275

Total: ~\$525, or about \$1.05 per foot. Using individual pricing yields a savings ~\$0.20 per foot.

While straight pricing typically favors unbundled product, factory bundles reduce labor cost. A rough rule of thumb is 2 or 3 hours preparation time per 500 feet for bundling cables oneself, which saves a few hundred dollars to DIY.

## **Factory Bundled Pros & Cons**

While more costly per unit length, factory bundled cables take no time to assemble together. Aside from improving install speed, having a single bundle of wires make hiding and protecting the cable easier than separate strands.

However, multiple variations of bundles are available, and proper specification is essential. Furthermore, not every door uses the same 'mix' of devices, and the bundle may change between openings. Additional, depending on the installed location of door components, individual cables may need to be run separately from a bundle regardless.

## **Installation**

Running cables to door and access components is frequently more difficult than standard ethernet networks. Not only are the overall number of cables greater, the locations they run to are often farther away and in difficult to access locations. Also, the construction of doors and frames vary greatly, and running cables 10 feet at the door can be more time consuming than running hundreds of feet in cable trays or raceways.

To conceal and protect door cabling, it must often be run through door and even window frames. Take the example of a common glass 'store front' type opening, composed of swinging thin framed glass doors and 'lites'. Rather than taking the shortest route from controller to components, a longer path crossing multiple panes and frames must be taken, extending overall cable lengths and installation times.

Care must be taken when drilling into frames to not break glass, and fishing cables in tight spaces is a manual and time consuming process. Take the example storefront below, and notice the cable path must cross multiple frames to reach secure mounting locations:



## Other Factors

Access control cabling can encounter atypical constraints. For example, access cabling is frequently run in direct contact with metal frames, and some AHJs may require more stringent insulation specifications (e.g., rigid tubing/ conduit or thicker jacket) than standard types.

Another common issue is required penetration of firewalls to connect devices. In many cases, cabling is run to avoid drilling or cuts through a rated wall, but this is unavoidable with access control installation. Drilling through a wall may require [a fire-rated connector](#) and the use of a [fire-rated sealant](#) to back-fill any holes.

Prior AHJ approval to make a penetration may be required with subsequent inspection of the final cable run. Since requirements vary by jurisdiction, [checking with the AHJ](#) is a prudent first step.

## Wireless / WiFi Access Lock

For some access openings, running wires can add thousands in cost, and wireless alternatives that avoid it becomes appealing.



But using wireless and WiFi locks can have drawbacks over hardwired alternatives.

We examine key aspects of both types, including:

- The differences between Wireless and WiFi access
- WiFi Drawback: Power Hungry
- Wireless Drawback: Lockdown Feature Often Difficult
- Repinning locks is often still needed
- Battery costs can be hundreds per year
- Replacement Costs

### WiFi/Wireless Locks Defined

By design, WiFi/Wireless locks are frequently a single standalone door lock with key tumbler and one or more integrated credential readers. An internally stored database of users and

schedules in the unit usually makes capable to provide access without network connectivity present (albeit without being able to update the database or monitor entrance).

A WiFi/Wireless lock can be installed much quicker onto existing standard door lock cutouts than a traditional hardwired access system composed of multiple pieces that must individually be hung and wired on the opening.

The image below shows this contrast:



WiFi/Wireless can also be used to network individual access components like [Door Controllers](#) and [Access Readers](#) as well, although that implementation is not as common.

### Wireless or WiFi?

When it comes to potential problems, it starts with defining exactly how locks are networked together. Two major distinctions are common, with units using:

- Proprietary wireless
- WiFi

## Proprietary Wireless

Proprietary radio networks limited to the lock, usually in the 900 MHz - 2.4 GHz range require a system hub to be located in the range of every lock. The hubs range between \$200 - \$500 each, with coverage of about 500' in any direction, line of sight.

Common types of proprietary wireless include:

- Assa's [Aperio](#)
- Schlage's [Engage](#)
- Alarm Lock/Trilogy [Networx](#)
- PDK's WiMAC (Zigbee Pro based)
- Z-Wave Plus (Yale, Kwikset, and many residential locks)

See the example Zigbee Pro based wireless used by [ProdataKey \(PDK\) Access](#):



## 802.11 WiFi

With units using IEEE 802.11 WiFi connections, the lock is given an IP address.

With WiFi locks, existing WiFi networks generally can be used, with insignificant bandwidth impact.

Common types of 802.11 WiFi locks include:

- Assa's [Corbin Russwin or Sargent Locksets](#)
- Allegion's [NDE and LE](#) (Can be optionally deployed as Engage connected)
- August's [SmartLock Pro](#)
- RemoteLock [Products](#) (including '[ResortLock](#)')



### **WiFi More Expensive**

Usually, WiFi units are more expensive per lock. However, the additional cost of adding specialty radios for a separate network can easily bring deployed cost well above WiFi cost.

WiFi locks are typically not limited by a hard maximum on the number of devices added to a network, only limited by the number of concurrent connections a WiFi network can maintain.

Which protocols are used impacts deployment of central hubs or radios and can impact how far away and how many units are controlled.

For wireless systems, the limit is often twelve or sixteen units, but multiple hubs can often be 'teamed' together for high-density applications.

## **WiFi/Network Security**

In most cases, concerns about WiFi locks being detected and hacked beyond the range of buildings is offset by using encryption, generally a minimum of 128 bit AES.

Moreover, most WiFi locks use whatever WiFi protections and configurations an existing network is already configured with, and the locks themselves are just another networked device.

However, the true 'protection' of the encryption used by these locks are often not scrutinized. In many cases, the primary buying criteria for customers buying wireless locks is to lower cost, and their potential security risks/impact may not be understood.

## **Repinning Locks**

In many cases, hanging a WiFi/Wireless lock also means replacing the mechanical locks in use.



In order to remain useful with existing keys and keying systems, new locks need to be pinned to comply.

While the cost of repinning a lock may be less than \$20 and is likely good for years of use, this initial expense is frequently overlooked and can be hundreds of dollars for a system of a modest number of doors.

### Battery Costs

In large deployments, maintaining battery power in locks can cost hundreds or even thousands per year. While most lock vendors pin internal battery life at many tens-of-thousands of cycles, battery life is calculated under optimal operating conditions and doors.

Consider if a single lock requires a (\$50 parts/labor) battery pack replacement once per year, a system composed of just ten locks will cost \$500/year.



The type of battery power a lock uses may range from a specialty battery pack or the lock may be designed to use standard commercially available replacement batteries, but in either case, batteries will cost money not needed by hardwire powered locks.

Even a slightly misaligned or worn door may experience some drag or binding on the door lock. This additional force to overcome can quickly drain internal batteries.

The orientation and use rate of the door can greatly impact battery life, with an occasionally used opening lasting longer than one used heavily. If the interval between power draws is

several minutes or longer, the battery pack has time to recover to full voltages between cycles, while one used constantly will drain quicker because of constant use, but also because the chemical recovery of cells is intermittent.

### **WiFi Locks Use More Power**

In general, the type of radio used also impacts battery service life.

A drawback for WiFi units is because they remain in constant contact with access points, they often drain battery life rapidly compared to low-power wireless Z-Wave/Zigbee that use intermittent contact.

Additionally, the lock's distance from the radio or hub can significantly impact battery life, with locks farther away and with a weaker signal trying to re-establish a connection or find the network more often.

### **Wireless Lockdown Not Always Available**

However, a drawback for wireless (i.e.: not WiFi) access: time-sensitive commands like emergency lockdown may not be available.

The intent of that function permits a central alarm or user to simultaneously lock all doors in a system, potentially restricting access to potential threats like active gunmen or other unauthorized users.

With any wireless system, network reliability and speed are a concern. With 'Lockdown', this concern is amplified because an unresponsive or slow lock may leave innocents at risk.



Confirming a wireless lock system includes 'lockdown' features are the first step, but also designing the wireless network and maintaining radios to the degree the command is acted on quickly is the next.

If little tolerance is allowed for a potential failure of a lockdown command on a specific door, wireless/WiFi locksets should not be used at all.

### Replacement Costs

Finally, if lock parts break, will replacement of the whole lock be required? Unlike a hardwired door with many discrete components, if an auxiliary device breaks or malfunctions, it can be swapped out.

With a wireless/WiFi lock, if a routine wearing part like a keypad or deadbolt wears (costing less than \$100 USD normally), the entire unit often needs to be exchanged at a cost of \$1,000 USD or more.

# Drain Wire For Access Control Reader

An easy-to-miss cabling specification plays a key role in access control, yet it is commonly ignored. The drain wire offers protection for readers and controllers, ensuring proper cable performance.



We examine the drain wire, the role it plays, and why it should not be ignored.

We cover:

- Why the drain wire is needed
- How to identify the drain wire
- Why access readers make them mandatory
- Why only one end is connected
- How much drain wires typically cost

## Drain Wire Purpose

The data exchange between reader and controller can be corrupted, subject to environmental interference from other sources or even building materials like steel studs and door frames.

Given that reader wire typically is run to devices installed outside buildings, but connected to controllers deep inside them, the length of cable connecting them can attract and trap potentially degrading electrical/ EM interference that corrupts analog Wiegand or RS-485 signals between devices.

Unless the conduit between reader and controller, or controller to head end is shielded, low-level problems are difficult to diagnose and troubles can result.

### **OSDP Use Of Drain Wires**

The data format used by the reader and the controller changes the drain wire's importance. For analog Wiegand or RS-485 serial, the drain wire is critical. It is less important for digital OSDP.

OSDP's digital format is more tolerant of the interference that can make Wiegand unreadable. However, because most OSDP readers can function in Wiegand or RS-485 modes as well, installation instructions often include using a cable with drain wire as well.

The vast majority of readers installed use Wiegand, but as the overall adoption of OSDP increases, the mandated use of the drain may become less important.

### **Identifying Drain Wire**

The drain wire is an unjacketed copper-tin conductor that is bundled in jacketed cabling. In the image below, the drain wire is indicated as it typically is included in UTP bundles.



Essentially the drain wire provides a convenient manner to ground cable shielding, although the wire itself provides protection from Radio Frequency Interference (RFI) and helps reduce RFI emission from the cable.

### **Shielding Is Not Grounding**

The drain wire is installed connected to the [Ground](#). Importantly, the wire is 'groundable' to a screw tap, and grounded cable runs are not easily installed when only a shielded foil jacket is available.

In many cases, STP cable specs also include a drain wire for the purpose of grounding the entire shield. But even for non-shielded cable, a drain wire alone may be specified in order to ground the cable.

For more on grounding, check our: [Grounding and Bonding for Video Surveillance](#) tutorial.

### **Specified Explicitly**

Drain wires must be specified explicitly when ordering supplies as they are not always included in standard cabling. Even if one orders shield cabling, drain wires are not always included (See our primer: [STP vs UTP for Surveillance](#)).

### **Access Readers Typically Require Drain**

While a 'fine print' specification, drain wires are typically required by EAC devices like card readers, door controllers, and other devices where data is exchanged. A drain wire is commonly included in the pigtails attached to readers, and the use of that wire is required in instructions:



Because its importance is not always appreciated, drain wire specifications are commonly overlooked. As a result, when cable shielding is specified, it frequently is installed improperly. The simple presence of a foil jacket or braid within a bundle does not shield the cable against all interference unless it is properly grounded.

### One Wire End Connected

The most common question asked when working with the drain wire is "Which end of the wire is grounded, or are both ends connected?"

Among manufacturers, there is no consistent answer. Below, we show several excerpts from installation manuals, with some manufacturers even changing instruction between models:

**IPVM** | **Drain Attachment Instructions Vary**

**Device #1: AWID**

For the remote antenna wire, use ALPHA 1294C (22AWG) 4-wire, stranded and shielded cable. The cable shield drain wire must be grounded at the reader end to P1, pin 4 connection (DC Power Supply Ground).

**Device #2: IEI**

Connecting the Reader to the Host:  
Connect the reader to the host according to the wiring table below and the host installation guide.

Wiegand	Wire Color
+ DC	Red
Ground	Black
---	Violet
Data0	Green
Data1	White
Shield Ground	Drain
On/Off LED	Orange
Red LED	Brown
Beeper	Yellow
Hold	Blue

**Device #3: Linear**

**Device #4: HID**

Note: Use Ground (GND) for the drain or tie it to the reader ground if the reader is not powered off of the module (5 VDC reader).

**Device #5: AWID**

**Sentinel Prox LR-911**  
**Installation Practices and Procedures**

**AWID**

**Wiring and Power Supply**

**Common Wiring Mistakes**

Failing to connect the DRAIN to the Shield or Drain of the connecting cable. Connecting cable should NOT be tied to Ground at either end.

The examples above illustrate a number of options:

- *IEI #2*: Connecting the drain wire at both ends of the run
- *AWID #1 & HID #4*: Grounding at the reader
- *Linear #3*: Grounding at the controller
- *AWID #5*: Nonspecific which side, just that drain should be grounded

In order to be effective, the drain should be grounded at one end to allow potential effects to 'drain' away from the shielding. For more on electrical grounding, see [Grounding and Bonding for Video Surveillance](#).

However, not all instructions call for one end to be tied to the ground. Rather, some devices are designed with grounded connectors on the board or in the device's pigtail and instruct both ends to be connected.

## **Added Drain Cost**

When added to cabling, including drain wire adds a modest cost. Depending on the accompanying shield specification, the price increases between 25% to 45% per foot versus unshielded/no drain wire products. Per door, this generally adds about \$10 to the cabling price.

Given the low cost involved, not including or installing the drain wire to spec can result in greater long-term costs in tricky troubleshooting and unreliable systems.

# PoE Powered Access Control

Powering access control with Power over Ethernet is becoming increasingly common.

However, access requires more power than cameras, and the problems of not having enough are significant, especially if unsecured doors, unresponsive doors, or dead readers are the result. Considering access impacts life safety, special effort needs to be taken to ensure that mistakes are not made in powering.

We teach:

- Why PoE for Access Is Useful
- PoE versus PoE+ Use For Controllers
- Why 4 Doors Is Typically The Max PoE For Controllers
- How To Calculate PoE Power Load For Access
- How To Check Available Field Power
- The Code Impact Of Using PoE
- Cost Savings From PoE Powered Access
- 4 Common Problem Areas When Using PoE Powered Access

At the end, take the 7 question quiz on PoE Powered Access Control to test your knowledge.

## Where PoE For Access Is Useful

PoE is useful in retrofit access control to bring power to the door, instead of installing high voltage electrical for the system first, an expense that can often cost hundreds of dollars per door.



Without PoE, power at the door involves extending or running new circuits from breakers to openings in new conduit with new outlets, power supplies, enclosures, and junction boxes, while PoE routes power through the same cable that connects door devices to an ethernet network.

### PoE Overview

Central to using PoE for Access, and undoubtedly any application, is understanding how much power is available.

Two major types of PoE are commonly used:

- *802.3af* supports up to 15.4W and is used by most PoE enabled Access Controllers.
- *802.3at*, 'high' PoE, supports up to 25.5W but used only by a small fraction of security equipment, generally those designed to be used in extreme weather environments.  
However, 'at' is compatible with equipment specifying 'af'.

In access control, 802.3at use is not common, but some controllers may offer a version using it for higher output or pass-thru ratings for powering high demand locks or readers. For example, [Paxton offers a 802.3at Net2 unit](#) that offers 1.5A/20W of output:

## NET2 PLUS WITH POE+ POWER SUPPLY IN PLASTIC CABINET



Electrical	max	units
Output voltage	13.35	V DC
Output current (PoE+ 802.3at type 2)	1.5	A
Output power (PoE+ 802.3at type 2)	20.4	W

For more on PoE, both as a general resource and a surveillance features, see our [PoE Guide for IP Video Surveillance](#).

### PoE Into Controller and Out to Access Devices

The typical access architecture is for PoE to directly power the [door controller](#), with the controller powering attached low voltage access control devices like readers and in some cases, locks. The controller consumes some of the PoE power as overhead for its own operation, but then passes on portions of what is left to companion pieces. Usually this power is divided up to the different ports based on the device type connected to it.

### PoE Controllers Frequently Limited to 4 Doors Or Less

Controllers with four or more openings using PoE are uncommon, for the simple fact that while the controller itself is powered, the remainder amount available 'passed thru' to field devices divide in four partitions is too weak to power the locks and readers.

Unlike IP cameras, where a single device draws power from a PoE source, with access control, controllers supporting PoE are just the first device in a chain. Most PoE sourced power is exhausted just from the controller and devices composing one or two doors. As a result, PoE options are common for single or double door IP based controllers like Mercury EP-1501, HID Edge EVO, and the Axis A1001.

## Field Powering Attached Devices

Three main types of devices receive power from the controller - readers, locks and door sensors. How much power these devices need total is critical in determining whether PoE will be sufficient for each opening.

- *Readers:* The most common device receiving direct power, most keypad or card readers are specified to operate on steady power sourced only from the controller.
- *Locks:* Depending on lock types, using controller pass-through power may not be optional. For example, while Strikes may be able to operate off of PoE power budgets, Maglocks typically cannot as they draw significantly more current.
- *Door Sensors:* In some cases, other sensors may draw power from a PoE supplied controller for door position or even RTE, but this is not commonly needed or used.

In many cases, the total power needed for all these devices will exceed what PoE is able to provide. As a result, totaling up all the individual power requirements and reconciling against the supplied power is critical for every controlled opening.

## Three Steps to Calculate

First, check what type of PoE the door controller accepts (e.g., 802.3af or 802.3at). Next, verify how much output power max the controller provides. Then compare to the total power consumption needs of all devices being power from the control.

### *Workable Scenario*

In our first example below, more than enough power is available:

A door is controlled by a [Mercury Security EP1501](#) supporting 802.3af PoE, and passing through a max of 650 mA to field devices. To that controller, a [HID 6005 Prox Reader](#) requiring a max of

75 mA of power, and a [HES 8300 Strike](#) needing 240 mA on a continuous duty basis are connected and draw power.

The total power demanded by the reader and strike is 315 mA from the controller, compared to 650 mA provided, which is more than enough.

#### *Failed Scenario*

However, in this second example below, notice how insufficient power is available.

A door is controlled by a [Mercury Security EP1501](#) supporting 802.3af PoE, and passing through a max of 650 mA to field devices, To that controller, [two Aptic MTK15 readers](#) (for a read in/read out application) drawing a max 230 mA each, and a [Folger Adam 310-4 Strike](#) needing 510 mA on a continuous duty basis are connected and draw power.

The total power demanded by the readers and strike is 970 mA from the controller, exceeding the available power by over 300 mA despite no warning or connection obstacles otherwise.

#### **Available Field Power**

Check the specification sheet of the controller to determine how much power is available. For example, this [HID controller spec sheet](#) lists the following power values:

Output Power (MAX) for individual field devices, DC Input = PoE	
<b>Wiegand / C&amp;D Reader</b>	7.1W (580mA @ 12.25VDC)
<b>Wet Output (@12VDC)</b>	6.9W (580mA @ 12VDC)
<b>Wet Output (@24VDC)</b>	8.6W (360mA @ 24VDC)

According to this chart, the maximum available field power for particular devices vary by port. For example, the 'Reader' connection offers up to 580 mA for a device using 12.25VDC, or about 7.1W.

For 'wet outputs', or contacts that provide pass-thru power to control a lock, notice the desire output voltage affects the output amperage and wattage as a result. While this particular controller offers either 12 or 24 VDC selectable outputs, not all controllers do. Neither will all controllers divide up or limit pass thru power to a particular port. In many cases, the controller portions max power between reader and output ports, but other controllers simply assign a controller max field power output for all ports.

### Max Power Varies

Another key point is how field power amount varies based on power source type. Typically when using PoE for power, overall available power is less than what is possible with separate low voltage power supplies:

Output Power (MAX) for total system (all field devices)	
<b>DC Input @ PoE</b>	9.6W
<b>DC Input @ AUX +12VDC</b>	14.4W
<b>DC Input @ AUX +24VDC</b>	28.8W

Note that the total power available with PoE (9.6W) is 33% less than 12VDC (14.4W) and 66% less than 24VDC (28.8W).

### Code Impact

Many designers avoid using PoE to power locks outright, even if adequate power budget indeed is available. Building codes may complicate using PoE for power. Perhaps the most common issue is found for "Request to Exit" Pushbuttons that release door locks when pressed. The most applicable code, IBC 1008.1.4.4.3(2015) defines:

*"A manual unlocking device (push button) shall result in direct interruption of power to the lock – independent of the access control system electronics.* When the push button is actuated, the doors must remain unlocked for 30 seconds minimum. The push button must include signage

stating "Push to Exit" and must be located 40" to 48" vertically above the floor and within 5' of the doors. Ready access must be provided to the push button."

This code basically prohibits controlling lock power by way of contact closure on the controller, and mandates a direct break in lock power through interruption. At the very least, a push button must be installed in series between a PoE source and a door lock, but many AHJs reduce this to 'full power must be cutoff', even at the supply source as to be fully 'independent of the access control system electronics'.

For those looking for formal code citations online, see [Free Online NFPA, IBC, and ADA Codes and Standards](#) for area relevant versions and actual code language.

### **Cost Savings Significant**

Using PoE to power doors often save ~\$200 - \$250 per door, given the elimination of extra cable, power supplies, and labor. For example, one could eliminate:

- 500' of 18/2 Power Cable: \$90
- 4A 12/24VDC Power Supply: \$50
- Installation Labor for Above: \$60 - \$100

Compared to an average door cost of ~\$1,000, this savings can be quite significant.

### **Potential PoE for Access Problems**

Even when properly applied, PoE can present operational issues that separate power supplies do not. For example:

- *Low-Draw Strike Bind:* Many low power strikes, especially those marketed for PoE use, are vulnerable to misalignment jamming and binding that full power, high draw models can simply power through. While PoE is not the root cause of these issues, systems using PoE locks often require more frequent adjustment and are more sensitive to typical wear.

- *Maglocks*: Because maglocks require continually duty power and are relatively high-power locks, many PoE controllers are not built with contacts rated for continuous use. Intermittently powering strikes or deadbolts are within design limits, but continually issuing amperage at supply limits are not. Warnings against powering maglocks directly from the controller, by way of PoE, are commonly stated.
- *Backup Power Drain*: In addition, if PoE is used, the demand and subsequent drain on battery backups can be substantial. If the doors fall unlocked when power goes out, then specific high-availability backup power may be more prudent than a general resource used network wide. In many cases, breaking out access control PoE devices from other general networked devices is too complex for backup power management, and physically separate power supplies may simpler and less costly to manage.
- *Reboot/Updating PoE Switch Kills Power Supply*: A member explains "When doing a switch firmware update, PoE power is lost. When it is a camera system, the inconvenience is merely lost video during the upgrade. When it is access control panels, the penalty can be unintentionally unlocking or locking doors." The problem is caused by the system falling dead during <routine> firmware updates, but also then not negotiating PoE again when the update brings the switch back up. To mitigate the risk, PoE UPS devices can be applied, often for ~\$200 per opening to bridge the 'power gap' while a switch is temporarily offline.

## Quiz Yourself

Take the [PoE Powered Access Control Quiz.](#)

# **System Design and Special Conditions**

## Access Control Specification

This 15 page report provides the most in-depth guidance on specifying Access Control systems you will find.

Specifying Access Control correctly can be tricky, because every opening has quirks and are prone to outside factors that impact system performance. Not only this, but what you don't specify can be just as problematic as what you do.



Most access RFPs have serious problems. While they comprehensively spell out contract conditions and business terms, they are typically scant on relevant details about the system. Not only do they tend to be a random smattering of technical points, pulling them together into a cohesive system is often needlessly costly or may even be impossible to build.

### The Big Mistakes

Most of the trouble specifying access has a root cause in one of the three areas below:

1. Incomplete details, where things you don't know can ruin your budget and system goals.
2. Difficult to build, where details that sound prudent may actually limit selection and significantly drive complexity to integrate.

3. Proprietary, where even generic boilerplate writes in choices that lock you into one vendor.

We address the best strategies to avoid these problems.

### **Doing It Right - 18 Key Specification Areas**

The good news is that you do not need to be an expert to specify great systems. In the sections below, we cover the right details to include, how to include them, and how to avoid common traps through addressing these 18 areas:

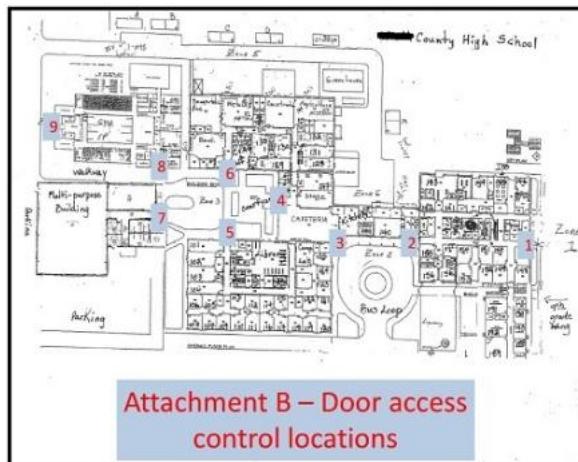
- Is This An Expansion or New System?
- Determining Access Security Goals
- Establishing Monitored, Managed, or Forensic Use
- Identifying Other System Integrations
- Which Credentials To Use
- Defining Doors/Opening Detail
- Defining Turnstile Use
- The Importance of Door Position Switches
- Defining Existing Locks/Hardware
- Specifying Readers
- Deciding to Use IP or Serial based Controllers
- How To Use PoE For Powering Systems
- System Edge vs. Centralized Architecture
- Is System Networking Wired or Wireless?
- Considerations For Using Existing Databases
- Evaluating User Management Features
- Using Special Features Like Time and Attendance & Mustering
- Establishing System Maintenance Expectations

First take a look at how common mistakes appear:

## Common Examples

RFPs for access control might be well intentioned, but that does not mean they will get the job done. Look at these examples we pulled from recent RFPs:

*Not Enough Detail:* With any specification, the risk is including too many particulars that potentially drive cost. However with Access Control, the opposite is more typically true. Take this example from the Specifications section of [this school's access solicitation](#):

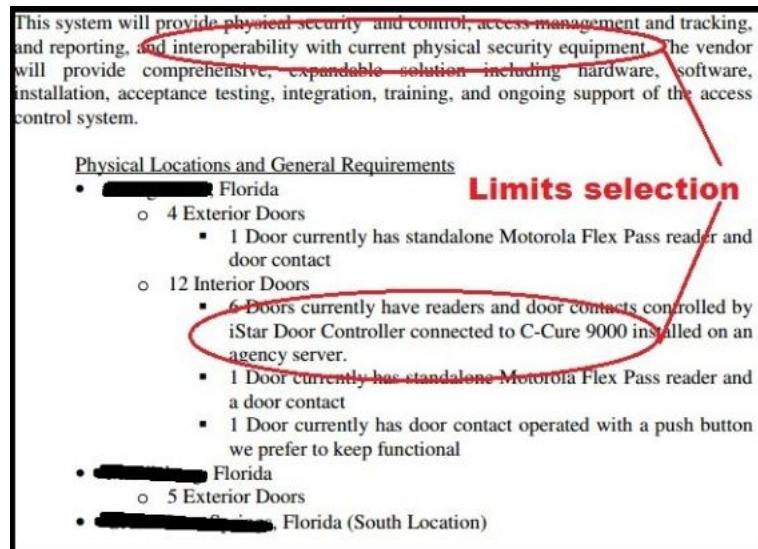


## Woeful Specifications

The bulk of details to build a quote from are found in the map above. No details regarding door/opening type, existing hardware, how many people need to have access or what credential types they carry, or when the openings should be unlocked are noted. Not to mention that descriptions of how and who the system will be used, or which other systems will need to integrate with the access platform.

Granted, all these details may be released or discovered after a job walk, but not all respondents may have a fair crack at using them to build a bid.

*Careless Specification:* Another regrettable trait is the inclusion of specs that sound smart or economical, but prove to essentially limit choices to just one or two bids. Take the example from a Police Department RFP:



### One Specification Excludes Most Choices

Overall the spec includes good detail including door descriptions and locations and is non-biased. However, due to the ambiguity in defining 'interoperability' and the listing of a single proprietary type of door controller essentially limits quotes to expansions of that existing system.

Whether this is intended or not is difficult to guess, however it would be much more efficient for both the solicitor and the bidders to state this requirement plainly upfront. The author does not realize the proprietary nature of access systems, they may think they are economically trying to use existing hardware for another system. However, the lack of detail defining 'interoperability' dooms this option.

## Technical Specification

Here are 18 technical aspects to include in every access specification:

## **Defining Expansion or New Systems**

Is this system new, or will it be a scaled addition to an existing system? Divulging this upfront will clarify for all involved what kind of work is being scoped. Due to the proprietary design of most access systems, interoperability is essentially non-existent, and if a system is already in place and satisfactory the best path is likely expanding that platform. This is likely the least expensive option since redundant equipment like servers and software may be avoided an not needed.

Also making this plain potentially avoids mistakenly buying two systems that cannot incorporate each other's equipment. Even if the goal is abandoning an existing system, recovering or reusing some of the existing components is a goal that should be made clear from the start. Special labor or software tools may be needed to transfer existing cardholder information, a point our "[Replacing Access Control Systems](#)" note elaborates in more detail.

## **Security Goals**

Harder to define, but essentially important, is to give a concise explanation of the goals for the access system. Stating "With this system, our facility wants to restrict off-shift staff from entering the premises and keep all but certain individuals from entering <specific areas> at any time" will greatly assist those designing a system in knowing the important features to build around.

Specifically, when access control is confronted by the issue of "Tailgating", knowing where the most sensitive openings are located is key when specifying equipment to offset the risk. For deeper definition and detail on this risk, see our [Tailgating: Access Control Tutorial](#) note.

Even when specialty design or equipment is not needed, establishing the rough groups that get access and when/where they need it is the foundation of access control. Making these basic goals clear will help bidders select the right platform with the proper level of assignable features for the stated need.

Restating and examining these goals when expanding an existing system is still essential, as the areas of control and vulnerabilities can change over time. Including a short statement describing 'security goals' can refresh the effectiveness of a system even decades old.

### **Monitored, Managed, or Forensic**

Next is to define how the 'control' aspects of the system will be managed. Is the goal to set everything up initially, and then only access it when absolutely necessary? Will an onsite guard staff actively monitor and respond to events 24/7/365? Or is it better if system oversight and monitoring is active, but farmed out to a central station facility?

Defining just how the system is going to be used and by whom can control costs by avoiding unused features, or by making sure the right people can manage the system at the right time.

### **Other Systems Integration**

Do you want your access control to be combined with video surveillance or intrusion alarms? Do you have a fire alarm system? Making a point to state these goals, complete with the current make/models/versions of the systems to be integrated help drive design and installation labor requirements.

### **Credentials**

If the system is new, important decisions should not be answered by the lowest bid response. If an expansion of an existing system, the answer might already be made. However, in either case, explicitly defining which credential type is desired prevents it from being a purely economic decision.

In terms of technology, most access systems use contactless credentials. In the past, 125 kHz credentials have been the mainstay, but due to security concerns (lack of encryption) and limited storage capacity, they have been superseded by 13.56 MHz types. From a cost standpoint, the more advanced credentials are the same price or cheaper than older formats.

If no credentials already exist, deciding the right product is as much security design as an economic one. How many people will be credentialed? Should photo IDs double as badges, or is a more durable option needed? What other systems use credentials, and should they be combined? What about biometrics? Does risk mandate multiple factors are used?

Additionally, if existing facility codes are in use, they should be noted as a specification of the future system. Not all systems are able to work with dynamic codes, and this minor detail may drive significant cost if not made clear.

For more details, read our reports on:

- [Access Credential Form Factor Guide](#)
- [Fingerprints for Access Control?](#)
- [Multiple Factor Authentication Guide](#)

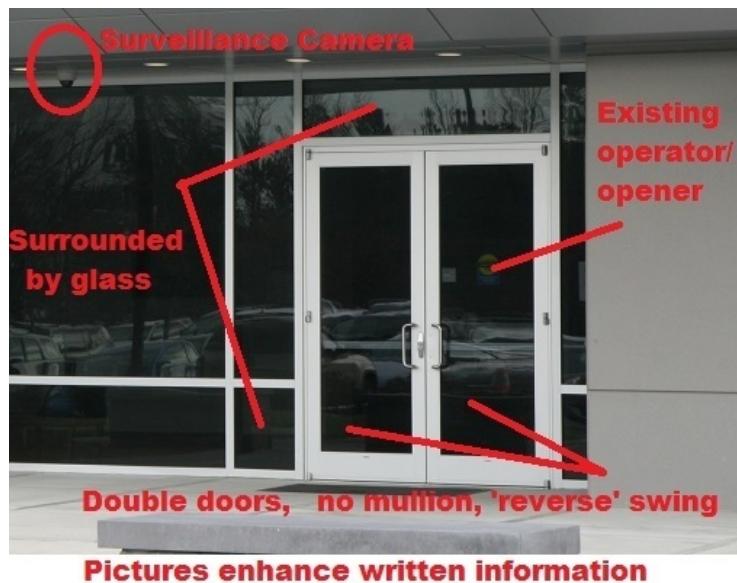
### **Doors/Openings Detail**

Describing the openings to be controlled is helpful not only from a design perspective but also from potential management changes. No two openings are alike or used the same way, and a short description or picture of the opening and it is used goes far in designing good controls.

For example, the 'main entrance to an office building' is better described as this:

*"The main entrance is a set of glass double doors that both swing out. These doors are handicap accessible, and the right side automatically opens and closes when a nearby button is pressed. A nearby security camera should be integrated into the system so that all potential users are recorded as they enter. This entrance is typically used by the public during business hours, but should be locked and only accessible by approved users from 7pm - 6am overnight.*

*Approximately 30 people may need access during a typical night during those hours, including cleaning staff and delivery people. This picture shows the opening:"*



Note: Photos need no annotation, just a good clean shot of the opening to be useful.

While not technical, the information provided gives great insight that cannot be observed during a quick job tour and includes door type, door function, security goal, user volumes, and secondary system integration (video). While expert knowledge is not needed, passing on basic details mitigates guesswork.

For more detail on how to properly describe openings, whether they are doors, gates, or even turnstiles, catch the readings below:

- [Door Swing Primer](#)
- [Glass Doors and Access Control](#)
- [Turnstiles Guide](#)
- [Gate Access Control](#)

### Door Position Switches

One of the most useful, yet most neglected aspects of access control are the sensors that indicate whether the door is shut or open. While many view DPS as an 'extra', there remains no

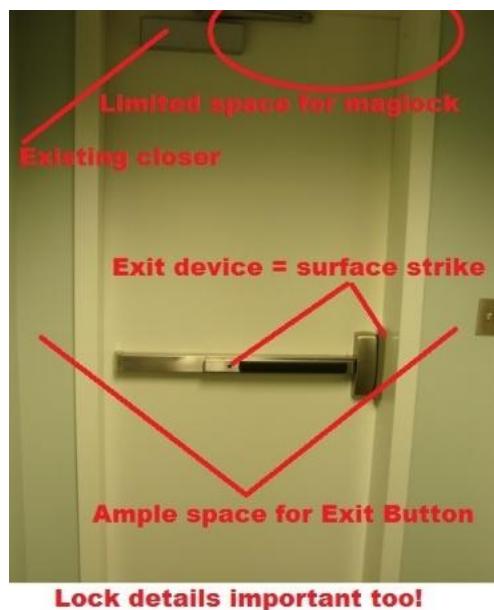
more effective or inexpensive way to monitor the current state of the opening that these sensors.

Since they are viewed by some as 'optional', solicitors should explicitly state they want these sensors included. Catch our "[Door Position Switches \(DPS\) For Access Control Tutorial](#)" for more detail. For insights on the biggest barrier to successful use of DPS switches, read "[Combating Door Prop Problems](#)" to catch the subtle behavior that totally undermines the access system.

### Existing Locks/Hardware

Like doors, expert-level detail is not required, but basic observations are useful. Often access control interoperates with existing mechanical locks, and quick inventory of how each opening is appointed is invaluable to choosing the best method of control.

For each door, a picture or basic written description is useful: "*The back door is a metal (steel) door currently kept closed with a panic bar. The door swings out and has an 'Exit' placard above it. The door can be locked or unlocked from the outside of the door by a key only issued to managers. See picture for details:*"



For further details on describing locks or how to choose the right type for securing your access door, see these posts:

- [Understanding Lock Functions](#)
- [Specifying Door Locks](#)
- [Maglock Selection Guide](#)
- [Electric Strike Selection Guide](#)

## Choosing Readers

Selecting the right reader is the result of which credentials are used and where the opening is located. From the written descriptions and photos of the doors/locks, good decisions can be made what type to include and where.

Clearly indicating the openings where [Multiple Authentication Factors](#) should be used help ensure the right reader is specified to support all credentials needed at that spot.

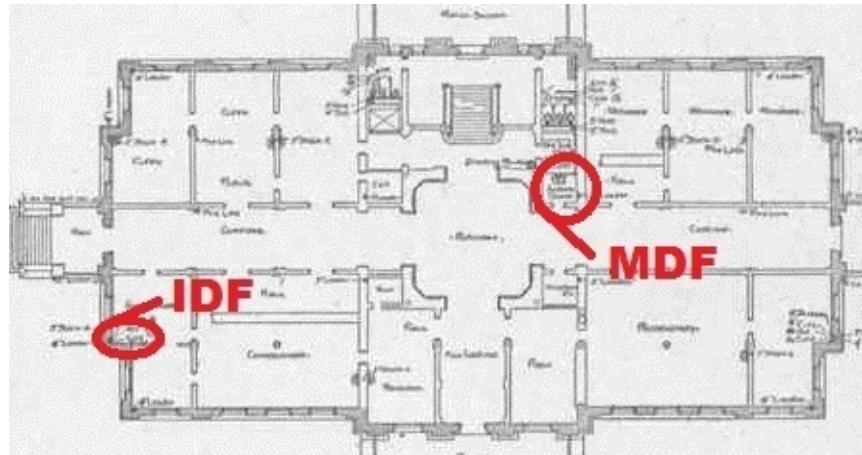
For general background and more detail on choosing readers, catch our guides below:

- [Access Reader Selection Guide](#)
- [Keypad Reader Concerns](#)
- [Proximity Readers Tutorial](#)

## IP or Serial Networked Systems

The network that ties a system together should be mentioned if existing cabling or LAN should be used. Hard specifying one type over the other can be costly if preference is not strong, although many modern systems use IP networks as the primary option, a trend that will continue.

If existing networks are to be used, making the locations of existing switch rooms clear avoids guesswork or expensive redundancy. Marking a set of floorplans that include these positions part of your specification is vital:



## Network /Server Room Locations

If new or dedicated networks are needed, making note of any raceway, main cable trays, or access panels confirms that new cable will run concurrent with existing.

### Edge or Centralized Architecture

To a lesser extent, specifying where door control takes place is important. Most modern systems use a form of door controller mounted near the opening, and specifying centralized location of system components could significantly drive cable costs or result in older systems being bid.

Even if 'edge' systems are used, all equipment can be installed behind locked closets or secured enclosures. However, making sure enough space is allocated for those devices is commonly overlooked and can drive costs if not properly considered during spec writing. These reports include more detail the subject:

- [Controllers or Control Panels](#)
- [Securing Access Control Systems](#)

## Using Power Over Ethernet

In many cases, standard 802.3 af/at PoE can be used to inject power to edge controllers and subsequently connected devices like readers and strikes. Using PoE is generally more convenient and offers online management when separate, stand alone power supplies typically do not.

However, using PoE may limit the range of connected devices based to 'total pass-through' power available, which is usually 750 mA or less, and the max number of doors on a single PoE powered controller are limited to two. Other factors to consider include the rating of the controller contacts, and disclaimers against powering maglocks on a constant basis from a PoE controller are common.

Our [PoE Powered Access Control Guide](#) includes an in-depth look at the subject.

## Wired or Wireless

When it comes to controlling cost, hard specification of wired systems can cause prices to skyrocket for remote or hard to reach openings. Especially if those doors are not heavily used, but electronic control and logging is essential, consider using wireless and 'stand-alone' styles of locks.

While the unit cost may be high for a single wireless lock, the overall cost of connecting multiple devices together via a long network run could be more expensive. While the overall price and maintenance associated with wireless locks (ie: replacing batteries) could be prohibitive for entire systems, they could prove an economic fit in lieu of significant wired network expansion. For more on these applications, see our "[Wireless Access Primer](#)".

## Using Existing Databases

Especially for larger, multi-site systems, the database can bring significant cost. Assuming the most economical choice will be made is foolish unless the specification explicitly states which database platform may already be available. Our "[Hidden Cost of Access: Database](#)" posts covers this point, and the common options, in depth.

## User Management

Defining user's needs are a critical aspect of the specification, and one where presuming features will be available is dangerous. Spelling out expected 'Live View' and management control helps designers specify what can configure the right platform. If operators need to lock/unlock doors in real time, weekly activity reports are to be created, or if the access system should integrate with the video surveillance system, these requirements should be clear.

Even for systems that are not actively managed, if items like 'remote access' from smartphones or inclusion of 'ID Badge' creation modules, it should not be assumed it will be included unless stated.

Also, if specific workstations are to be used for running clients, description of their location and build specifications should be listed so deploying the system to operators is confirmed. For more details on the software management piece and explanations of the typical features desired, see the following posts:

- [Access Management Software Guide](#)
- [Maintaining Access Records](#)

*Special Features:* Access control is useful for more than just unlocking doors. Many systems include options for 'Time and Attendance' logging that essentially replaces a time clock, or 'Mustering' that grants you special reporting that provides a roster of occupants in a particular area.

If these features are desired, or any other integrations falling outside the core access control functions, effort should be spent defining the desired result in specification documents. These posts will help clarify what to ask for and how to note the requirements:

- [Time and Attendance Tutorial](#)
- [Mustering Tutorial](#)

## Maintenence Costs

Finally, specifications should spell out any ongoing annual software maintenance costs and any additional ongoing expenses required to keep the system current and operational. Some platforms have no ongoing maintenance plan, while others require a yearly plan and may not prioritize service or tech support if not current.

The cost of this maintenance should figure into system selection, as a system may be thousands less when initially installed, but add thousands in unrealized costs in subsequent years.

## Access Control Specification Form

The following section provides a summary of each requirement and common options to consider. We recommend you copy and paste this into your own documents and use it as a starting point in defining the requirements for your access systems.

**Opening/Door Type:** Often best depicted in a picture. If not permitted, a short written description describing: Steel, wood single or double door? Right, left, or swing ‘reverse’. Glass opening? Turnstile?

**Users per Hour:** Average number of users during busy times, so that cycle times of locking hardware can be sized accounting to the busiest period the door permits access.

**Opening's Security Goals:** The high-level purpose of access control: “Restrict unapproved users from entering during overnight hours” or “Only residents with current rent payments should be allowed to use gym facility.”

**Other Equipment on the Door:** Often best expressed in a picture, a snapshot or written description of the other hardware devices hung on the opening. Examples: “Closer on upper hinge side, vertical rod on upper strike side, and an exit device hung on the inside. Outside keyed access.”

**Reader Type/Mounting Position:** On the door frame (mullion), or on an adjacent wall? Are mounting surfaces suitable? Are they protected/sheltered from ice and snow? Can someone in a wheelchair or with limited range of movement reach the reader, per ADA (or similar)?

**Credentials to Use/Multiple Authentication Needed:** Common Choices: 125 mHz, 13.56 MHz contactless. HID format, MiFARE/DESFire? 26,33,34,35 bit cards? Facility code needed? Is more than one credential needed at the door to verify the user?

**Intercom Needed?:** If a user cannot enter the door, or if a visitor request entrance, can they page help or an attendant? Two two-way conversations need to be supported?

**Lock Type Needed:** Choices- typically electric strikes or maglocks, but dictated by building code, AHJ preference, and type of hardware existing on the door.

**System Network Type:** TCP/IP, Serial hardwire, wireless, or stand alone locks? If IP, are existing LAN segments available? Are cable pathways and data closets marked? If wireless, the signal strength at doors verified?

**Controller Types:** Choices- Edge or Centralized? Standalone or host dependent?

**Critical User Management Features:** What real-time features required? What type of reporting is needed? Will users need access from a browser or mobile devices? Are client workstations available?

**Server Space/Preference?:** Do you have available resources in the server stack? Are they physical or virtual? Do you need your servers to host access locally or remotely? Including this

ensures no ugly incompatibilities happen at the last minute. If a new server is used, will local IT resources be familiar with configuration and support?

**Database Platform Needed:** Does your enterprise already use a standard database platform like SQL? If so, make note so the access system can plan to make use of existing rather than purchasing new or using a proprietary platform.

**Special Features:** Do you need Time & Attendance or Mustering? If so, does your hardware design support those features? Make note of the 'other systems' you would like access control to feed into or use like video surveillance or intrusion alarm.

# Access Control Mustering

In emergencies, determining where employees are located can be critical for knowing whether they are in danger. Access systems can be used for reporting employee locations, also called 'mustering'.



We examine the strengths, weaknesses, and cost of using access control for mustering, including:

- The two types of mustering used with access
- Manual 'check-in' assembly point kiosks
- Using mobile readers for flexibility
- Why area tracking often breaks code
- Contrasting costs for both mustering types
- Why stand-alone 'real time' systems perform best

## Mustering's Main Goal: People Accounting

For all methods, the goal of mustering is to account for specific individuals, so if they are not confirmed present within an area, additional action can be taken to investigate where they are.

In an emergency situation, the resources to search for the unaccounted are limited, and having an accurate list of who is present helps bring focus to those efforts.

### **Access Control For Mustering**

Access systems typically use one of two methods of mustering:

- Manual Check-In: Less expensive to implement, but less accurate reporting
- Area tracking: More accurate reports, but more rigid and costly to implement

### **Real-time Mustering Uses Standalone System**

The third type of mustering is typically not part of access systems and is typically a separate system that uses phone apps, non-access control RFID credentials, and standalone databases.

This provides high accuracy and real-time location data but uses active power tokens/cards.

### **Personnel System Integration Useful**

How integrated mustering reports are with other systems like Time & Attendance and [Visitor Management Systems](#) are a factor in how useful they are.

Commonly, access mustering reports are not deeply integrated with other systems. So when names do not show on mustering reports, finding out where they are located requires manually calling or checking out with managers to see if PTO, sick leave, reassignment, or break times mean they were out-of-place but otherwise accounted for off-site.

These 'off-line' efforts take time, and quick response is crucial in emergencies. In our experience, mustering reports are not deeply integrated but serve as a 'start point' list of names for local managers.

However, highly integrated systems use inputs from time off, reassignment schedules, and time & attendance systems to make quick work of determining who is a priority to find. In these

cases, the names not appearing on a muster list are excluded because the people are otherwise accounted for.

### **Manual Check-In**

The most common approach for mustering is to implement a simple 'opt-in' control, using an access control reader located at an 'assembly point' or evacuation area that is scanned as cardholders congregate in that location.

The list of names is then compared against the assigned list of evacuees who should scan into that reader during an emergency. The risk is when employees do not manually scan in the kiosk, they are not reconciled in the system and may be in danger.

The image below is an example mustering point with external reader kiosk:



The cost of installing kiosks includes \$1,000 - \$1,500 for the kiosk itself, and additional costs of trenching or wirelessly connecting the kiosk to the access system.

### **Area Tracking**

Area tracking is the more expensive and complex mustering method using access scans to generate a roster of occupants in a certain area.

Every time an occupant scans a card to enter and leave an area, the access system logs the time, date, and credential holder of the credential and users are 'subtracted' from an area as they scan out.

While this data can be used to determine who is in the area at any given time, accuracy is more difficult as users may not always scan out when leaving an area.

Where life safety/ egress codes permit, mustering accuracy is maintained by scan in/out turnstiles, often requiring physical modification of entrances and training users on safe operation:

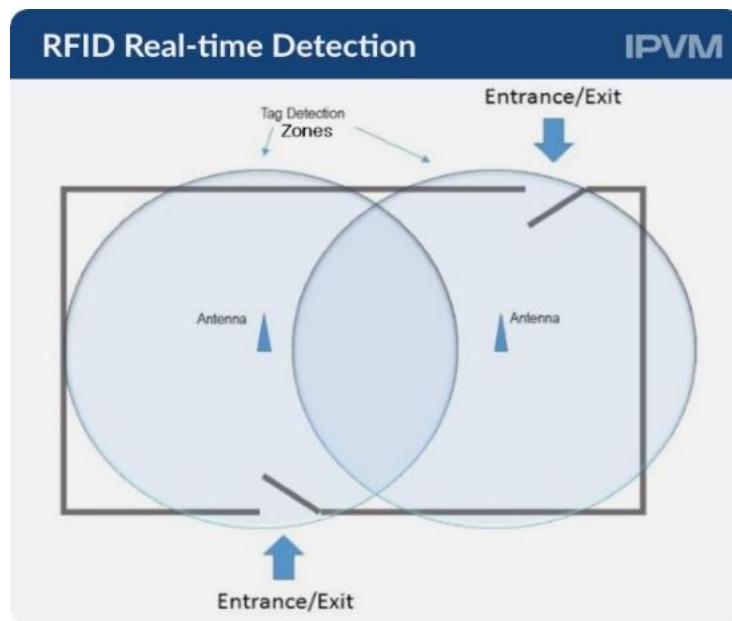


However, this need to restrict egress in order to enforce 'read-out' is often not allowed and is illegal in most public/commercial [Building Occupancy Codes](#).

Pricing of controlled entrance/egress points vary, but often range from ~\$3,000 - \$5,000 per opening [if turnstiles are used](#).

### Real-time tracking

The third type of mustering is typically not integrated into access controls, using a wireless network to detect where a user's powered credential is located:



With these systems, deployment costs usually mean issuing credentials to all users and wireless radios in all areas, which can be tens of thousands of dollars for a typical commercial location.

Providers in this niche include [Cybra](#), [GuardRFID](#), and [S3-ID](#), but many platforms and solutions are market-vertical specific and the 'best' solution often varies based on how/where it is used.

### **Where Is Mustering Used?**

Aside from 'Emergency Roll Calls', mustering functions can be applied in several ways. In industrial or mining facilities, mustering can be used for 'Lock Out/ Tag Out' situations, where machinery should not be restarted or an area reoccupied until all maintenance personnel is accounted for.

Likewise, in facilities where frequent headcounts are essential, like prisons, daycares, or passenger manifests, mustering can be configured to ensure that all members of a group are present in an electronically logged system.

Depending on how mustering is implemented, it can send notifications or print reports to predefined locations. Not only can 'absentee reports' be sent to nearby printers within an

evacuation area, it can send emails or text messages to current occupants alerting them to emergencies (i.e., severe storms, bomb threats, or other emergency circumstances).

### Mobile Readers: Hybrid, Limited Solution

A lower-cost hybrid mustering solution is to deploy totally mobile wireless battery-powered readers for use during evacuations at assembly points.

In general, a few trained 'managers' carry these readers and are trained to scan evacuee badges as they arrive at assembly points.

However, one major limitation of these mobile solutions is that they must be used within a fixed wireless range of a hub, often ~500 feet, which may not be far enough to be safe in an emergency, or otherwise range can significantly decrease by shelter wall construction.

Commercial systems range in price of [~\\$1,500 - \\$3,000 per reader](#), with most access credential formats supported.



# Tailgating

Nearly all access control systems are vulnerable to an easy exploit called 'tailgating'. Indeed, a friendly gesture in holding doors for others often compromises access security.



We take a look at 'tailgating', the most common causes, and contrast 5 options to address/minimize tailgating:

- 'Hold Open' Alarms
- Turnstiles/Revolving Doors
- Mantraps/Airlocks
- Piggybacking Detectors/Analytics
- Signage & Vigilance

## The Problem

'Tailgating', also called 'piggybacking', describes the situation when a credentialed access user opens a door allowing one or more individuals to immediately pass through while the door is open.

The situation can benignly occur when holding a door open for someone. It also happens accidentally, typically when someone is focused on hurriedly making it through an open door.

Rare, but most risky of all, is when someone commits a malicious act by purposely sneaking behind a valid cardholder to beat the security system. Tailgating's impact can render an entire facility insecure.

### **Common Courtesy The Biggest Enemy**

In many cultures, holding the door open for people is a warm, kind expression. Likewise, explicitly slamming the door shut behind you is perceived as rude, and can create ill will between neighbors or co-workers.

However, many people do not consider how they are undermining an access control system with their own 'good manners'.



Indeed, many cultural objections to not holding a door often circulate. Countless articles decrying the failure of civility are popular, like:

- [A question of etiquette: do you hold the door for others?](#)
- [Men, Hold The Door Open For Women](#)

- [Here's The New "Holding The Door Open For People" Rule](#)

However, the aspect these articles fail to recognize is doors are only secure and protective when closed and locked.

### **Security Awareness Is Key**

Many people do not deliberately seek to undermine the physical security of a room or building, but they fail to recognize how risky their behavior can be.

The best method to balance 'politeness' with 'security' is reinforced awareness of why, or if, a door is a security point. Not all facility doors, not even those frequently used, are necessarily part of the security access controlled perimeter. But if a door is kept closed and locked, or if it is equipped with access devices like readers or keypads, it should never be held open and politely kept closed after authorized entry.

For these openings, user training and door signage is necessary to reinforce security importance. Training people and hanging signage is 'low tech', but often effective way of dealing with this risk.



### **Other Contributing Factors**

There are a variety of other tailgating root causes. Understanding the 'why' of each door threatened helps to determine the best defense against it:

- **Bad Weather:** Especially in rainy and cold climates, holding the door open offers a welcome shortcut to those seeking the warm and dry environment of a facility. In these cases, sheltered entries, [windbreaks](#), or awnings help diminish the tendency to hold open doors out of environmental harshness.
- **Misaligned/Worn Doors:** Over the course of thousands of open/close cycles, even commercial grade doors, hinges, frames, and closers sag or become worn over time. If left unchecked, doors may not fully close when opened or may take a long time to close, therefore allowing many people entrance from a single card read. A regular and discipline door maintenance schedule for access-controlled openings is critical to prevent the issue.
- **Inconvenience/Laziness:** There are a variety of simple ways to keep a door from latching after it has been opened. Doorstops, rocks, bunched-up rugs, and hardware tampering are all commonly employed to eliminate the task of presenting a credential for access, often seen as onerous by employees. For this reason, consider embellishing 'smoking area' doors or delivery entrances with cameras and intercom systems to mitigate tampering and provide other communications paths for outside access.
- **Malicious Intent:** Preventing untrusted or dangerous people from entering an area is often the primary goal of access control. Often, readers and locks alone are not enough to mitigate this risk despite the occurrence being minor. To properly prevent undetected entry, often additional engineering controls like sensors, analytics, or even turnstiles are needed.

## Tailgating Solutions

The risk of tailgating is widespread and almost every access controlled facility is vulnerable. Fortunately, a host of engineering controls are available to combat the problem. In the section below we take a look at the major types:

- 'Hold Open' Alarms
- Turnstiles/Revolving Doors

- Mantraps/Airlocks
- Piggybacking Detectors/Analytics
- Signage & Vigilance

### 'Hold Open' Alarms

Many access control systems have the ability to monitor door position switches - simple contacts that check whether a door is closed or not - and can be set to alarm if a door is held open for too long.

Alarming occurs on doors open longer than a few seconds, thereby indicating that multiple people are able to pass through a 'held open' door. However, while this is a low-cost or free measure for combatting tailgaters, it also is the biggest source of nuisance alarming when implemented. Unless a facility actively monitors its access control system, this solution is likely to be (promptly) dismissed as irritating and ineffective.

Externally fitted alarms usually cost between \$200 - \$400 however many access control systems can be configured to sound a local alarm via reader beeper and door position switches as a 'free' configuration setting.

### Turnstiles/Revolving Doors

In recent years, turnstiles have moved from massive, noisy mechanical devices to sleeker, quiet, architecturally styled access control points. This type of equipment restricts entry to a single person at a time and eliminates the ability to hold a door open for unauthorized access.

The promotional video below provides an example of an 'office turnstile' designed to restrict access into an interior space, and features 'tailgating' detection:

[Click here to view the dFlow video on IPVM](#)

We covered this particular unit in our [Free Flow Turnstile \(dFlow\)](#) post.

The cost of turnstiles and revolving doors can range from \$1,000 to \$25,000+ and are frequently core access features, not retrofitted afterthoughts. For more, see our [Turnstiles Guide](#).

### Mantraps/ Airlocks

These installations are entryways that feature two sets of controlled doors. Usually sized just large enough for one occupant, the doors are configured to open one set at a time.

This means the interior set cannot be opened until the exterior set has been closed and is locked. Because the physical space inside a mantrap is tight, only one person per card read is permitted through the doors.



These installations have a variety of operation uses beyond security; in some cases, they function as airlocks to segregate 'clean room' environments from outside contamination, or they are used as inspection checkpoints for contraband. These installations are expensive, often costing \$10,000 or more, and because they use multiple sets of doors and have large physical footprints, they are among the most costly anti-tailgating measures.

For more, see our [Access Control Mantraps Guide](#).

## Piggybacking Detectors/Analytics

This option, usually based in sensors hung on the frame of a door, in a floor mat, or nearby analytic-enable surveillance cameras, are configured to detect individual movement through an opening. The movement profile of a single individual is compared against the actual movement measured as it credentials into an opening.

We covered one floor-based sensor in [Anti-Tailgating Startup: Spyfloor](#) that detects multiple pairs of feet entering a door:



[Click here to view the animated gif on IPVM](#)

One example of the door-based piggyback detector show in the promo video below:

We also tested a video camera app analytic that detects people from overhead in our [Axis Tailgate Detection Test](#).



[Click here to view the animated gif on IPVM](#)

The cost of these solutions vary but generally range from ~\$430 for a camera analytic (less camera), to \$3,000+ for a single door detection mat or 'light curtain' sensor.

### Anti-Tailgating Vigilance Needed

While solutions abound, the 'best' option is a tough matter to decide.

Many security managers faced with tailgating simply rely on repeated instructions and signage to remind credential holders about the issue. Lacking the funding or organizational will to eliminate the issue, the vulnerability (and subsequent risks) of tailgating remain.

In many cases, little more than signs and vigilance are available to deal with the issue, but they can be used to good effect:



In those cases where tailgating must be prevented, the use of turnstiles and manways is common. However, due to the cost of these solutions, many end users find them too expensive and instead opt for less costly (and less-effective) options like Piggyback Detection or Video Analytics.

# The Passback Problem

Every security system has flaws, even high-tech ones. While Electronic Access Control helps keep sensitive areas safe, it is not without weaknesses.



One of the most troubling vulnerabilities is called 'Passback' - the practice of using someone else's credentials to gain entry. We take a look at the problem and how designers can minimize vulnerabilities, looking at:

- Passback vs Tailgaiting
- Software solutions including time limit and reader pattern and flow
- Other solutions including biometrics, cameras, turnstiles and signange
- Ignoring it

## The Problem Defined

'Passback' is the colloquial term for 'sharing credentials', taken from the example of two people passing through an access-control turnstile. Suppose 'Person A' scans their badge and passes through normally, but 'Person B' is not allowed access into the area. 'Passback' occurs when 'Person A' hands their badge to 'Person B' so that person can gain access.

This practice is roughly equivalent to slipping a door key through an mail slot to an outside person, or sharing your password with someone else. At best, it means that the system is not controlling access in the way it was designed, and at worst it could mean the system has no knowledge of a potential threat.

### **Less Risky Than Tailgating, Still A Problem**

In terms of security threats, [Tailgating](#) is a 'killer' risk, while Passback is generally less intense. Many passback events occur when people try to find ways to undermine the access control system, while Tailgating typically flatly ignores it. So in general, Passback is easier to manage with 'soft' methods or with direct reminders to users to avoid sharing credentials.

Simply defined, 'tailgating' means that once a door has been opened by a credential, it is left open so that more than one individual is allowed to pass-through. In contrast to 'passback', 'tailgating' simply bypasses the requirement to scan individual credentials. However 'anti-passback' controls, especially those of the 'Pattern and Flow' variety, may be able to combat the 'tailgating' problem.

For more, see our [Tailgating - Access Control Tutorial](#).

### **Basic Software Solutions**

To counter the risk, Access Control systems often feature 'anti-passback' controls, which generally describes a set of barriers applied to credential use. For example:

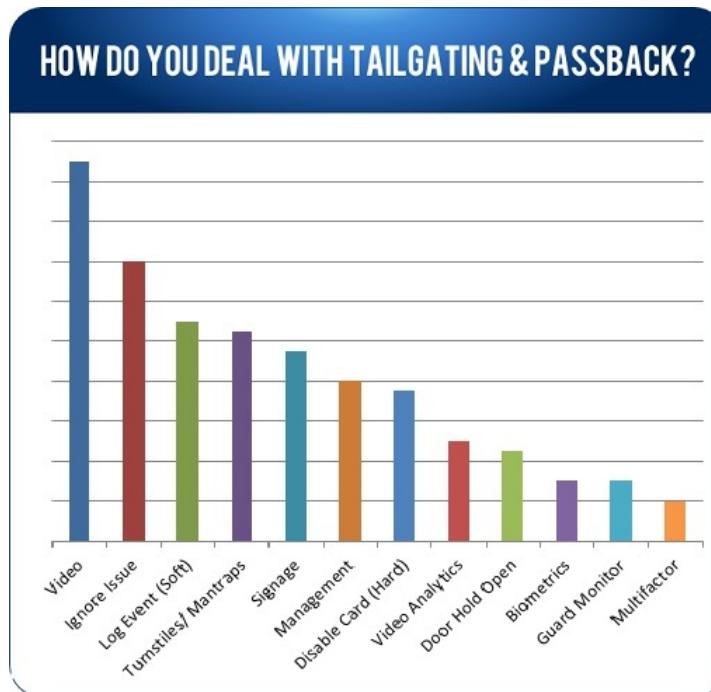
*Time Limit:* A card cannot be used at the same reader twice within a certain amount of time. While this represents a decidedly 'low-tech' solution, it is the easiest to implement. Simply limiting a card to be read on the same reader for a period of 3 to 5 minutes discourages the convenience of improperly 'passing-back' a credential. However, this type of control can be inconvenient to users, on the occasion they accidentally drop something after reading a card, become distracted by a conversation, or have some other legitimate reason for quickly re-credentialing through an opening.

*Reader Pattern and Flow:* This type of control requires credential reads follow a logical pattern within a system. For example, a credential must be used at an 'OUT' reader before it can be used for an 'IN' function. Likewise a credential cannot be used to enter 'Building B' if 'Building A' has not first been exited. This method of anti-passback is the most comprehensive at controlling the problem, but it requires the most configuration and places an emphasis on having all doors controlled within a facility, even doors that are infrequently used.

Time Limits and Reader Patterning are software features that some, but not all, access control management software supports. For other, more strict solutions, additional hardware sometimes costing thousands is required.

### Other Solutions

Conclusively battling passback typically involves more than only software. For example, in our [Practical Solutions To Piggybacking and Tailgating](#) survey, more than 10 solution types were voted, and more than 80% of those responses mentioned using more than one solution method:



The most common 'other solutions' besides basic software cited:

- *Biometrics*: A sure way to prevent passback is to credential based on biometrics instead of 'shareable' credentials. Tying access permissions to unique physical features generally stops most sharing.
- *Cameras*: Another common approach involved using surveillance cameras to record and verify no misuse was happening at access points.
- *Turnstiles*: The most common 'strict' method were using turnstiles, revolving doors, or mantraps to physically prevent more than a single person entry at any time.
- *Signage*: The most common 'soft' measure of those that indirectly or passively address the risk was the use of signs to remind people that misusing the system invites danger or undermines security controls.

### **Ignoring Piggybacking Risk Common**

However, another key trend identified in the results was ignoring the issue. About 15% of responses said they simply do nothing, because addressing it is too costly, or it is not enough of a risk to warrant countermeasures.

Choosing to ignore the threat may seem prudent for some, but doing so introduces the opportunity to undermine and even invalidate the power features that justify using electronic access control versus traditional mechanical keys and locks.

# Delayed Egress

We explain the code, share real world applications and installation issues.

The sections below cover:

- The Major Codes Allowing Delayed Egress
- But Some AHJs Forbid Regardless
- All Applications Specifically Limited By Code
- Fire Alarm Override Required
- Nuisance Delay Optional
- Real-World Delayed Egress Applications
- How It Is Implemented - Panic Bars, Access Control Systems and 'Exit Check' devices

## Major Codes Allow Delayed Egress

Surprisingly to some, both [IBC and NFPA 101 codes](#) permit delayed egress, if done in a manner that meets specific safety requirements.

While the [approved occupancy classifications](#) differ between the two authorities, they both allow for exit from a building to be delayed up to 30 seconds, but typically 15 seconds. In practical terms, this means when someone approaches a delayed egress opening and pushes on the exit bar, an alarm sounds but the door remains locked for a short period before unlatching and allowing them to exit.

## **But Some AHJs Forbid Regardless**

However, not all AHJs are accepting of this method even when it is code compliant. Locking people behind closed door for any period of time is deemed too risky and potentially deadly, regardless of code acceptance.

Several municipalities prohibit or heavily restrict use of delayed egress for specific occupancies. For example, [Maricopa County / Phoenix](#), Arizona limits use of these locks in most situations, contrary to IBC and NFPA 101.

## **Fire Alarm Override**

Another requirement: even if delayed egress is used, all doors must be made to unlock immediately when the fire alarm is pulled.

This override is included in order to mitigate the stampede or crushing risks for those trapped behind a locked door during a fire event or other emergency.

However, some authorities recognize that many emergency egress situations unfold without involving fire alarms. Active shooters, severe weather, and bomb threat evacuations can be hindered by delayed egress locks. AHJs often object to any delayed egress because of these concerns.

## **Nuisance Delay Optional**

Depending on which code authority is accepted, the person exiting may need to press on the exit bar for three continuous seconds. This time period, called the 'nuisance delay' helps mitigate accidentally triggering a delayed egress door by simply bumping the exit bar. If no delay is allowed by code, then 'pranking' the door by bumping the bar and running is a potential irritant and reduces the effectiveness of the annunciation to supervising staff.

## Real-World Delayed Egress Applications

Delayed Egress is valuable in certain niches. Take the following examples:

*Retail Stores:* Modern 'big box' retail stores are expansive facilities that require multiple emergency exit doors throughout the building. In the past, shoplifters have taken advantage of these openings, simply loading up with expensive merchandise and crashing through these doors to waiting vehicles for a quick getaway.

Delayed Egress helps counter this problem. If someone attempts to crash through an opening, an alarm sounds for 15 - 30 seconds before unlatching, allowing for store associates to apprehend the shop lifter before escape is possible.



*Daycare/Nursing/Convalescent Homes:* Another valuable place to use delayed egress is where the risk of occupant escape is high. For daycare and elderly care facilities, ensuring that clients are secured indoors is a high priority, and use of delayed egress on unsupervised openings is an invaluable tool.

## **How It Is Implemented**

The list of components needed for compliant delayed egress varies according to how it is implemented, but public notification signage is required to be hung [link no longer available] on the door regardless of the method.

*Panic Bar:* Delayed Egress can be installed on any opening, even if it is the EAC system does not control it. However, in most cases, substantial specialized hardware is required. Most exit device manufacturers offer a delayed egress equipment package that can be retrofitted to an existing opening but the installed cost of these packages range between \$2500 - \$5000 each opening.

*Access Control Systems:* Many access control systems can be configured to release locking hardware after a timed delay. However, some forms of controlling hardware are able to be overridden by mechanical hardware (ie: electric strikes), so additional door mounted devices, like an 'exit check' may be required. The installed cost of delayed egress on an access controlled door can range between a few dollars for a sign (\$2) to \$2500 to integrate an delayed egress lock and annunciation sirens.

*'Exit Check' Device:* Often a modified type of maglock, this device is tied into an exit bar or senses opening force to begin a timed countdown. After that period expires, that maglock releases, and the door freely opens. The installed costs of this option range from a few hundred (\$400) to several thousand dollars, depending on the amount of extra equipment required to bring a door compliant with codes.

# Propped Doors

Doors should keep 'bad guys' out.

One of the most basic problems with doors is people propping them open:

Even worse, door propping undermines significant investments in electronic access control. The issue is especially frustrating to building security because it is so common and easy to pull off.

We examine:

- Common reasons for doing so
- Eliminate the means for door propping
- Adding signage and education
- Installing specialty equipment

## The Problem Defined

Propping doors is not a difficult issue to describe. Whether it happens because of wood wedges, kickdown hardware, or even rocks, trashcans, or kicked rugs, preventing a door from closing makes passing through it easy.

The classic 'convenience versus security' problem is clearly demonstrated by a propped door. Whatever the reason a door is held open, it cannot lock or secure the space within. When this takes place on perimeter openings, like the main entry for buildings, any stranger can walk in and perpetrate crimes.

Granted, door propping is not an issue with every door. Propping doors that divide rooms, offices, or closets may not cause security problems, but propping a facility's access controlled openings is a nasty issue.

## Why it Happens

Since propping is so common, what are the root causes?

- *Convenience:* Closed doors are a barrier. Not only does it takes effort to swing open, needing to lock it with a key or credential card is especially a hassle. Especially when passing through an opening many times, or carrying a load with both arms, keeping the door propped open is a welcome alternative to constantly fighting a shut opening.
- *Climate:* Doors are propped when the room inside is too hot, cold, or air circulation is stale compared to outside spaces. Keeping a door open provides some relief, but at a big expense to area security.
- *Hardware Malfunction:* Not all doors are deliberately propped open. In some cases, faulty hardware like worn hinges or maladjusted closers can keep a door open and unlatched through neglect.

## The Solution

Solving the problem does not require exotic solutions and can be done by:

- Eliminating the Means
- Adding Signage/Education
- Installing Specialty Equipment

### **Eliminate the Means: Trash The Door Props!**

This simple step often yields the most effective result. Uninstall kick-downs, throw away door wedges, and move items like floor rugs and trashcans away from doors.

People seldom give much thought or effort to propping a door, so making it more difficult to use trash or common items to hold doors open has a big effect.



**Kick-Downs**



**Strike / Latch Tampering**



**Door Stops**

## Signage/Education

Making a point to emphasize keeping doors closed also is inexpensive. By hanging signs and (vigilantly) reminding occupants of the important security purpose of closed doors, the propping problem can be significantly resolved.

## Install/Configure Specialty Equipment

When more stringent action needs to be taken, or when the problem needs to be eliminated, specialty devices or access control systems can be configured to alarm. Regardless of the device used, the operation of anti-propping equipment uses a set of contacts and a timer. When the door opens, the contact break open, and a timer begins to countdown. If the door does not shut within a range of time (typically 15 or 30 seconds), an alarm sounds alerting occupants to the open door.

If for no other reason than to avoid the nuisance of alarm sirens or the attention of security guards, occupants learn to keep doors shut.

Some basic ways to do this:

- *EAC Integration:* Many Access Control systems support an 'anti-prop' function that works in conjunction with door position contact and the door controller to send an alarm when doors are open too long. However, this feature may have no 'local

annunciation' or audible siren at the door, and instead sends an alarm to the access control management console for attention. Addressing the 'prop alarm' falls to guards or operators working with offenders to stop the problem. Configuring this alarm on a door already installed with access control hardware is a no-cost solution.

## Door Closers

The importance of the door closer is overlooked in door prop problems. Most often, these devices use a spring or hydraulic arm to pull doors automatically closed after they are opened.



[Click here to view the animated gif on IPVM](#)

Door closers are specified according to pull strength, the type of door they are fixed to, and how rapidly/slowly they must operate. For more, see our [Door Closers: Critical Security Hardware](#) post.

The surrounding environment, like predominant direction of wind or balance of the HVAC system may also play a role in specifying and adjusting a closer to properly shut the door.

[Note: This guide was originally written in 2013 but substantially revised in 2017.]

# Access Visitor Management Systems

"Who are you, and why are you here?" Facilities that implement Visitor Management Systems hope they never need to ask that question to anyone, ever.



While access control goes to great lengths to make sure only approved personnel are able to enter controlled areas, they hardly ever handle 'temporary access' well.

For that, Visitor Management fills a niche and claims to do a better job than the old, proven clipboard sign-in sheets.

We examine visitor management systems, their common features, and how they are best deployed.

## Three Goals

For every visitor management system, there are three basic goals for the system:

- **Accountability:** No one is allowed to enter the site without first logging it. This guarantees that no unidentified person is wandering around a potentially dangerous or

sensitive site, but it also matches that visitor with a specific sponsor, typically a permanent employee. This makes sure that the visitor's business is directly tied to a meaningful task and often results in a fully escorted visit while onsite, increasing site security.

- *Visibility:* While ID Badges and access credentials may only be issued to permanent employees, most visitor management systems include temporary badging, good for printing inexpensive labels worn for a few hours that make it clear someone is indeed a 'Visitor'. If someone is observed onsite that has neither a permanent ID nor temporary visitor badge displayed, they very quickly can be identified by guard staff as potential intruders.
- *Quickness:* Large facilities may be faced with handling hundreds, even thousands, of visitors per hour. Especially for high-security facilities like military bases or critical infrastructure sites, quickly processing valid large volumes of visitors is essential for timely visits reduced service costs, and keeping tight appointment times.

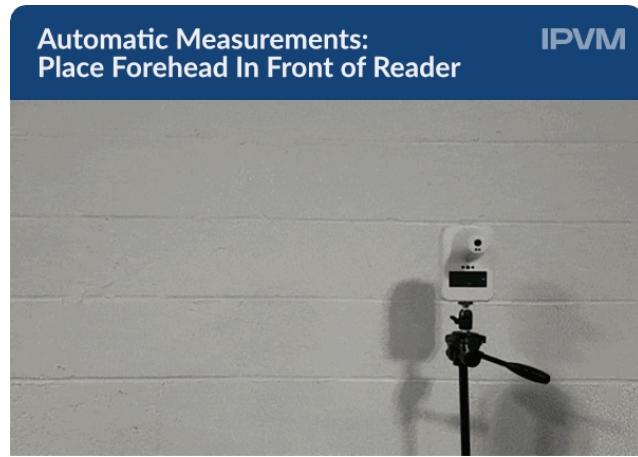
Additionally, most visitor management systems keep logs of visitor activity and the scope of why they visit.

### **Body Temperature Checking**

In the wake of Coronavirus, checking visitor temperatures has been added to many facilities. For this, thermal cameras, handheld temp guns, and body temperature tablets that also may check for face masks are common elements of allowing visitors onsite.

Because of the recent addition of this step to visitor management protocols, most systems do not support the step in the integrated process and it is often added by the user.

Even when non-handheld units are used, instructions to visitors often need to be very specific to mitigate read errors. The image below from our [K7 Wall Mounted IR Temp Gun Tested](#) report shows the typical process for visitors/users to approach a unit within close proximity:



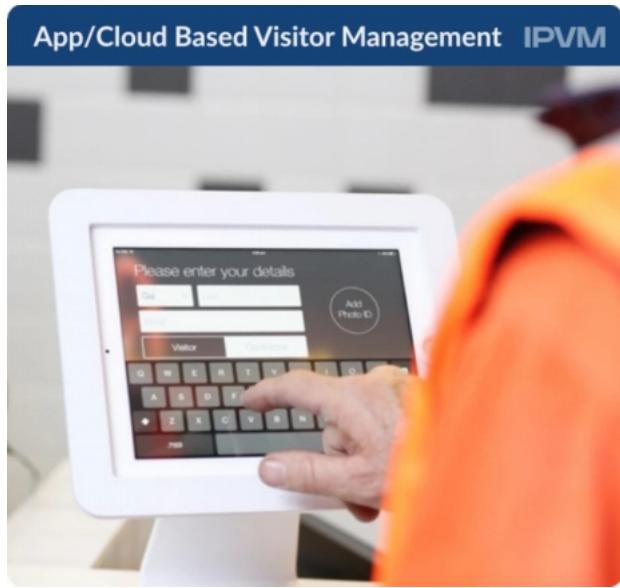
[Click here to view the animated gif on IPVM](#)

However, as our testing shows, the value of resulting readings is questionable especially given the range of variables that visitors, facilities, and test units themselves introduce into checking. See our [Directory of 400+ Fever Camera News Reports Globally](#) for more on how/where temperatures are checked, with many also questioning the true efficacy of it.

### **Self-Service Is Key**

A common aspect of visitor management systems is that they are designed to be used by visitors with only basic familiarity with computers. Visitors are often only prompted to answer basic details about themselves, with the integrated system working behind the scenes to provide access control settings, notify other users of activity/visits, and otherwise log the activity in the central access system.

Visitors are often asked to input details themselves, without intervention or need of other employees to manage the process:



Because of this, a variety of other systems, including physical access control, accounting, and vendor performance, may be integrated.

### Common Components

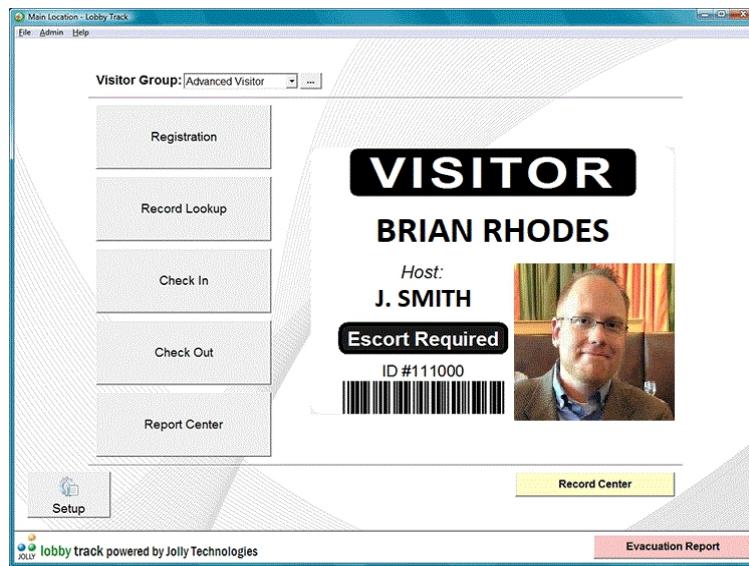
While the exact mix of hardware and software needed for the system vary, most systems use these basic components:



Here is an overview of each one:

### Workstation & Client Software

The central software is PC, tablet, or kiosk based, often networked to an access control management server, and most enrollment stations center around the data entry workstation.



From this point, visitors are 'enrolled' into the system, and often provisioned access permissions through specific openings or into controlled areas. This main console is where all the following peripherals are connected, as visitors often input their data or have pictures taken for whatever form of visitor credential they are issued.

### ID "Mugshot" Camera

A camera provides a visual record of a visitor, and even paper badge labels generally include a small black and white printout of the credentialed visitor. Some platforms use purpose-built 'ID cameras', while other systems use common webcams or even surveillance cameras to collect mugshot images.

## Paper Badge Printer

The end result is a temporary credential printed on a label marker. (See example below.) The composition of the badge makes the wearer's identity as visitor clear, and may include barcodes for provisional logical/physical access and include the expiry date.

The 'temporary' paper label visitor badges often resemble the example below:



## Barcode Scanner

If the barcode printed on visitor badges need to be enrolled in other systems, the enrollment station includes a reader to scan the badge into information or asset tracking systems giving the wearer provisional privileges to use access protected systems.

## D/L or ID Reader

In some systems, an optical or magstripe reader that can read general ID badges, like Driver's Licenses (D/L) or Government Common Access Cards (CAC) contain values that can be pulled into the visitor management system.



In many cases, the information collected by these readers/scanners is OCR'd or otherwise electronically transferred to a temporary visitor credential.

### System Costs

In general, the cost of a visitor management system includes software, hardware, and supply items like labels and ink. In some cases, Visitor Management may be a default (free) element of an access system, in other cases, it may be offered as an extra module, or it may be a 3rd party app.

The actual costs vary on the exact configuration and level of integration with other systems, but ballpark costs range about ~\$2,000 - \$5000 per enrollment station including all software, licenses, and peripherals/supplies. Some common platforms include:

- HID's EasyLobby: The most commonly used system, its cost ranges from ~\$2000-\$8000 per station (typically one per building). The price depends on the level of integration with mobile readers, cloud servers, and asset scheduling programs (meeting rooms, vehicles) or physical security systems like access control.

- Jolly Technologies 'LobbyTrack': With single-site cloud-based options running ~\$100/month, up to 'Enterprise' multisite network server-based versions costing \$8,000 Jolly's VMS integrates with many access control systems including AMAG, Brivo, DSX, Kantech, Lenel, S2 Security, and Software House C-Cure.

Other options are available as extensions or modules of ERP or Subcontractor Management systems, but the needed basic components are the same.

## **Applications**

Not everyone needs a Visitor Management system. Even facilities with aggressive access control may not need to implement visitor management beyond a well-policed clipboard system. However, the buildings that stand to benefit most from Visitor Management include:

- *Large Visitor Volume*: Where booking visitors require devoting labor hours to the task, a Visitor Management system can gain efficiency. With simplified data entry, sponsors doing 'pre-check-in' paperwork, and stored record access, sites can significantly speed up the process of getting visitors onsite quickly without compromising other security policies.
- *High Security*: Anywhere that places a premium on knowing the identity/business of EVERY individual onsite could use Visitor Management to make administration of the policy easier, and use the temporary ID badges to reduce the cost of credentialing every user.
- *High Liability*: Many sites contain dangerous locations. Furthermore, any visitor onsite may need to file proof of insurance or be recorded onsite to be covered by existing policies. Visitor management creates or manages these records.
- *Repeat Visitors*: In some cases, visitors are frequent guests. Rather than spending time every visit manually entering repetitive information, visitor management retains the information and can mean recurring visitors are able to conduct their business more efficiently.

# Time & Attendance

Access Control is useful for more than unlocking doors. One of the best features is also rarely used: Time and Attendance logging. However, selecting the 'same old' door readers for can open several vulnerabilities to abuse. In this note, we look at Time & Attendance Readers for Access Control, describe what features they should have, and what problems arise if they are not properly implemented.

## Time Logging is Central

One of the most powerful features of EAC is the time/date stamp associated with every event in a system. Not only do systems log when door opens, they also record whose credential was used to open them, typically down to the second.

Time Logging makes it possible to 'track' a user's movement through a system, and provide a concrete record of where a person was at a given time. These logs have even been used to [solve murders](#) and otherwise establish presence at certain times with high precision.

## Time Clock Function

With relatively minor adjustments, most EAC systems can use 'time logging' with [time clocks](#).



**Manual Time Clock**

**Time/Attendance Reader**

Many workers are paid an hourly wage. Clearly establishing when they start their job and when they stop working is crucial, as 'time' is indeed 'money'. Capturing this time has traditionally been the function of precise clocks, where workers insert cards to have the time indelibly punched out on a given day. Indeed, "punching the timeclock" is a common saying.

However, the method is not problem free. First and foremost, abuse is a risk, where an employee punches more than only his/her card. This type of fraud [is at the forefront of many HR and Corporate issues](#). Many seek to eliminate this risk/temptation entirely. While time clocks are primarily intended to protect the employer, the employee also benefits from having a clear record of attendance to lean on when calculating paid vacation days, sick days, or overtime pay.

Using the EAC system for Time & Attendance often means setting aside separate readers for the sole purpose of recording 'In' and 'Out' entries in the system. Once a pay period closes, a report is created listing activity on these two readers, summing the 'In' periods and subtracting the 'Out' intervals leaving an accurate record of attendance.

### **Multi Factor Makes Sense**

In order to avoid the pitfall of 'buddy punching' (a risk EAC systems normally call '[passback](#)'), Time and Attendance readers should feature multiple authentication factors, including fingerprint or palm readers. This 'extra authentication' ensures that no one can casually misrepresent themselves as another person.

Most modern EAC Time & Attendance readers feature biometrics, typically resembling the examples below:

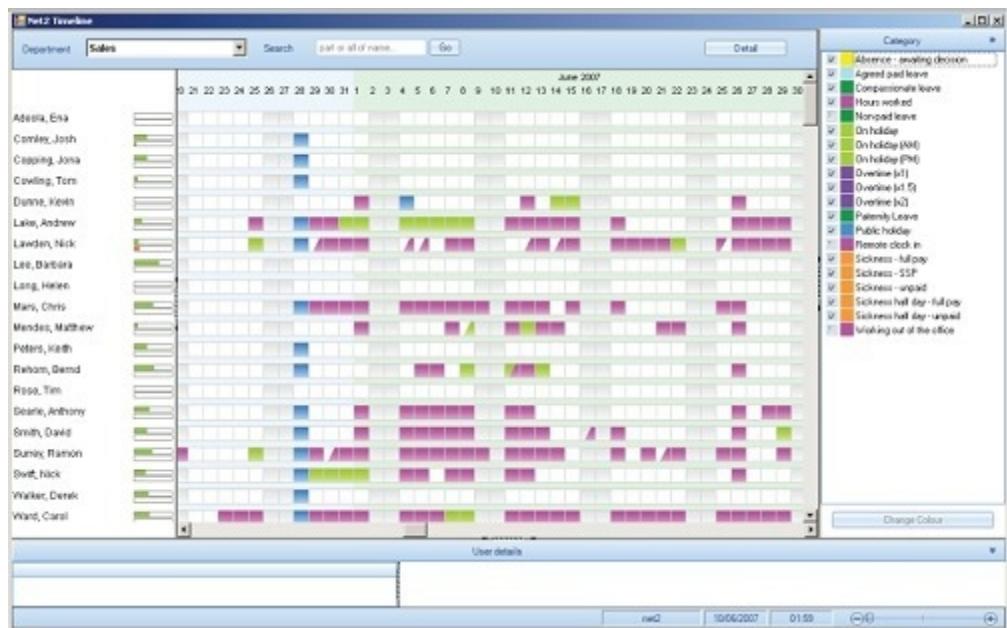


**Multifactor 'Time & Attendance' Readers**

These style of readers are sometimes sold as 'standalone' timeclock systems that require no EAC system interface, but this increases cost when connecting them with access headends. EAC systems simply need an interface to collect this data. General biometric access readers can be used in this role successfully (e.g., see our [3M/Cogent's MiY Touch](#) note for example).

### **Payroll Integration**

When EAC platforms market 'time and attendance' function, this is frequently more than generating custom reports. Many EAC systems will format data so it can be manually exported into payroll systems like [Kronos](#) or Sage. However, this is typically a manual process, and accounting or payroll staff require instruction on the access platform to collect reports. The screenshot below shows [Paxton](#)'s default export screen of Time and Attendance data:



In other cases, 'Time & Attendance' function may be based in the Access Platform, but an additional 'payroll module' is added to the platform for direct integration. This additional software becomes the default payroll platform, so adoption in large systems may need approval from 'non-security' stakeholders.

Common enterprise-grade platforms offer additional 'software module' solutions, including:

- [Lenel](#)
- [AMAG](#)
- [Software House](#)
- [Continental](#)
- [Honeywell](#)

## Costs

*Readers:* You could simply use a regular card reader but if you want to avoid buddy punching, time and attendance biometric readers range between ~\$300 and ~\$2000 each, with high-accuracy optical fingerprint readers costing around \$700 each. (See our [report on fingerprint](#)

[readers](#) for more detail.) Multiple readers may be required for large sites, and expanding the EAC system often includes adding controllers or interfaces to support those readers.

*Basic Software:* General costs to add a Time and Attendance module range from 'free' upwards of ~\$3000. Many platforms offer a '[no additional cost](#)' timeclock functionality to their basic system, but the data must be manually incorporated into a payroll platform.

*Advanced Software:* 3rd Party software / integration module provides more automated interface, but typically costs between ~\$500 and ~\$3000, generally depending on the size of a company's employee roster and number of sites data is collected. For most enterprise access systems, these modules cost about ~\$1,000 each.

## What are the Risks?

While using EAC to host time clock function can be advantageous, it is not without risks:

- **Clock Drift:** In effect, the EAC system clock serves as the payroll clock. While a variety of solutions for syncronizing/standardizing time exist, such as [NTP Servers](#) and central data clocks, differences between EAC and other timepieces can create significant problems. When EAC is used for Time and Attendance, keeping system time in sync with the local standard time is vital.
- **Single System Breakage:** Or rather '*Putting all your Eggs in One Basket*'. As a matter of redundancy, if your EAC system drops offline, so does your Time Clock. Why hiccups in granting access through offline doors can often be solved by issuing mechanical keys, no simple solution exists for Time and Attendance failover. You might want to have an older manual timeclock as a backup, just in case, and for the time the system is offline, manually reconcile the timeclock entries.
- **Passback Conflicts:** For access systems using 'Anti-Passback' controls, logic discrepancies can cause low-level conflicts with Time Clock readers. If an employee 'scans In' to the timeclock, and then immediately 'scans In' to a normally secured door, the EAC system may generate an alarm or deny access unless the timeclock reader is isolated from

passback rules. Given the large number of doors across multiple sites, or large populations of employees in a single system, these sort of errors can be common and hard to troubleshoot.

### What are the Benefits?

However, it makes good business sense to use EAC to host 'Time and Attendance' function, including:

- **Less to Buy, Maintain:** While a single system can be a weakness, it can also be efficient. Many facilities prioritize the upkeep of facility access systems, and issuing a credential for access also means it can be used for payroll. The investment in one facility system can be leveraged by another.
- **Expanded Security Controls:** In normal use, if an employee has a security credential revoked in an EAC system, they immediately become invalid in the payroll system. In addition, tying the two systems together can prevent an unauthorized employee from gaining access to an 'Time In' reader before an allotted shift and help manage overtime payouts, and payroll hour allocations are enforceable by physical access controls.

## Access Control Job Walk

Significant money can be saved and problems avoided with an access control job walk if you know what to look for and what to ask.



By inviting interested parties onsite for pre-bid job walks, many of the site conditions inadequately described in solicitations can be examined firsthand.

This detailed guide goes step-by-step explaining what to look for and ask, including key issues such as:

- The 4 key tools you need to take with you
- The 3 details you must note when reviewing each door
- The 4 things to look in access networking
- The 6 parts of access systems that typically can be reused in new systems

Finally, we conclude with a [5 question quiz](#) to test your knowledge.

### Four Tools Needed

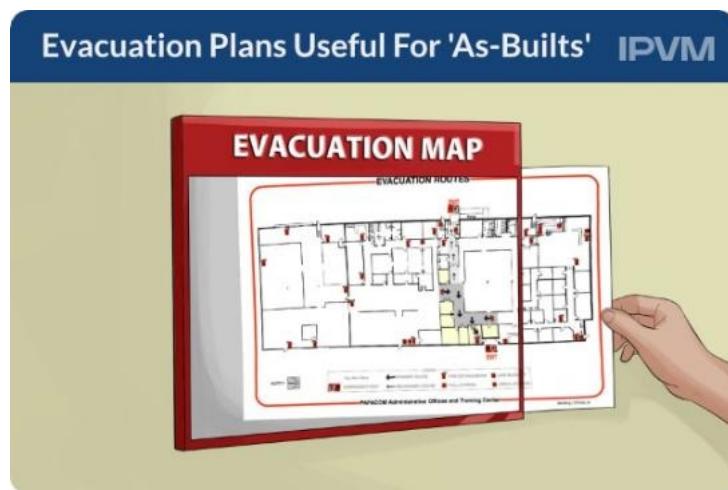
Having the right tools makes work more efficient and effective. A job walk's main purpose is essentially to gather as much information as possible in a short amount of time.

At the least, each job walk participant should carry the following items to make this time productive:

### Floorplans

In order to take detailed notes about the facility being controlled, a key document to have is a scaled drawing of the site.

If not provided in a bid package, a common source for workable drawings are in commonly posted 'Fire Evacuation Routes' in many buildings.



If no drawings are available, images from [IPVM's Google Map integrated camera calculator](#) can provide a good start for drawing design sketches. In any case, having these drawings before the walk begins helps recording important details a quick process.

### Measuring Tools

Physical distance and dimensions should not be guessed, as access designs often cover hundreds of feet and fractions of inches.



As noted in our [Measuring For Security Installation Guide](#), portable measures for length and location is best handled by a tape measure. Typical access measurements fall within the length limits of a 16' - 30' length tape, but occasionally distances (such as distances to server rooms or long cable runs) can be longer and require measuring wheels:



### Flashlight

Often access control ties into utilities or spaces not in plain view. Being able to clearly see into dark crawl spaces or attics is critical for paths to run cable or install controller panels is crucial.



Another key tool is a small hatband strap flashlight or handheld. Usually handheld LED styles using common battery sizes are best for access job walks, as they are small enough to carry and store in pockets.

### Cameras

Perhaps the most useful tool is a camera with plenty of storage for snapshots. Not every customer will permit pictures to be taken, so prior approval should be given, but when allowed there should be no reservation in photo documenting a site.



Both sides of a door (secured/unsecured), adjacent structural details like walls or windows, the area immediately surrounding the door including ceiling types, and any important details like

closets or server rooms should be photographed, as being able to refer to those details during bid development can be critical.

When in doubt, take more pictures than you may think you need, as it is typically difficult to return, yet there is little cost for having extra pictures.

### **Three Door Details To Look For**

During the walk, every future access control location should be visited and notes taken about how it is situated. Paying attention to how they have been designed and assembled at key points can greatly affect design.



Most often, swinging or rotating doors are the points of access control in a building:

### **Device Install Locations**

Access Control typically installs Readers, Locks, Controllers, and Cabling at a door. Mentally stepping through how and where each of these elements is installed is foremost in making the visit a success.

Having at least provisional knowledge of how installation tasks work and flow are helpful in understanding how site conditions impact system design. Taking careful notes and photos of how the opening is built means the best choice can be deliberated afterward and is not a snap decision.

### **Door Types**

For every door, the exact configuration and composition of the opening varies. Are you controlling a main entry, or is it delivery access? Will the door need to be opened and unlocked many times per hour?

Taking note of existing door hardware, special ratings like fire ratings, and the alignment/maintenance of the opening is important because it likely is not reflected in bid documents. Our [Selecting the Right Type of Electric Lock Guide](#) offers guidance for evaluating the right lock for a specific door type.

### **User Accessibility**

How will installed access equipment affect accessibility? Will a user on crutches, in a wheelchair, or with limited use of hands be able to gain access? If not, how will they be accommodated for? The answer may affect where equipment is located, but also which type of equipment is used.

### **Network Details To Look For**

Next, planning how the doors and devices should be networked together is needed:

### **Network Design**

Establishing utilities like cable trays, wire raceways and access panels typically make the job of designing networks easier. Instead of guessing where cable should be run, the decision has already been made but may not be clear in bid documents.

## Cable Pull Locations

Efficiently staging cable boxes/reels for minimum number of pulls can shave thousands in labor costs from a design. Accessibility is key, but planning cable pulls so that bends, turns, or terminations/connections are minimized ensures that overlooking a significant installation cost does not lose the bid. If staging cable reels or boxes in a hallway, will they block normal traffic? Or if the shortest cable pull runs overhead of an office or breakroom, will disruption be a concern? Being mindful of where cable should be run may also influence when it can be run, potentially impacting cost.



## Wireless

Even if no cabled network is installed, is wireless strength sufficient to reach and connect all wireless locks? Most wifi lock manufacturers offer a wireless survey toolkit that allows a quick check of signal strength at all doors. Logging readings at every location helps identify the gaps early before it becomes an operational issue.

## Panels/Power Supplies/Servers

Finally, checking to make sure that everything has enough space to be installed and is secure in those spots should be reviewed:

- *Mounting Real Estate:* Checking for open wall or rack space, or empty spaces above the door means no ugly surprises during install. Finding that there is not enough room to

mount central equipment can be an expensive oversight, and ultimately it may affect with type/form factor of hardware is selected. In the image below, six doors worth of access panels and related hardware takes up ~40 sq. ft. of wall:



- *Keeping it Secure:* [Keeping security equipment behind locks, alarmed, or hidden](#) should not be left to chance. Stepping through potential locations with system security in mind will protect the entire facility.
- *Power Tie-In/ Locations:* Confirming both availability and location of electrical service at the door or closets are important. While distance often can be addressed by cabling, the material and labor costs, and potential code restrictions are important to note before work begins. If approvals are needed to tie-in to existing utility, this should be done promptly rather than assuming permission exists.

## Upgrades And System Takeover

While not as common, some may be called to walk access systems slated to be changed or significantly upgraded. Taking inventory of which parts can be reused or which ones must be changed can account for thousands of dollar per door.

### Door Controllers

One of the costliest parts of an access system is the board or panel used to coordinate activity at the door. In many cases, the hardware used is proprietary to a particular system. However, the use of 3rd party hardware products is common, and even if not marketed that way. If controller equipment is sourced from Mercury Security, HID Global Edge/VertX, or Axis, there is a high possibility of connecting the opening in its current configuration to another 3rd Party Compatible management system.



Check our [Axis vs HID vs Mercury Access Controllers](#) post for more on potential reused controllers.

## Typically Reusable Parts

Other common components are typically reusable when connected to new access controllers.

While the cost of reterminating these devices into new devices should not be assumed as a 'zero-cost' activity (new cable may need to be run), these devices are typically compatible with access systems in default formats:

- *Readers:* Cards, fobs, PINpads, or even biometrics are often reusable if connected to controllers in Wiegand or OSDP formats.
- *Locks:* Basic low-voltage rate power supplies and relay contacts make lock almost always reusable.
- *Door Position Switches:* Simple sensors that monitor NO/NC circuit conditions are typically compatible with access systems.
- *User Credentials:* And finally, if the companion readers are compatible, then existing credentials often are as well, however confirming the format types with new system providers is a prudent step.

## Converting Databases

Finally, another substantial portion of access systems can often be partially reused, if not also requiring rework.



The underlying user database can often be exported and then imported into other access systems, preventing the manual data re-entry of thousands of records. The process varies, and in some cases specialized database translation tools must be used, but spending a few hours configuring a conversion process can save hundred of hours rekeying the same data into new systems.

### **How to Use the Findings**

Developing project estimates is a substantial topic all its own. However, for most jobs having multiple skillsets examine the collected findings is helpful to determine the best plan of action or installation path to address them.

Even the most experience designer benefits from a roundtable-style post walk meeting where the exact system design is established. Having multiple sets of eyes with different responsibility viewpoints means glaring mistakes and bad assumptions are less likely to end up quoted.

Also, having the full scope of trades review the data collected during the walk allows a clear understanding of where labor gaps exist. If advanced skills like finish carpentry or locksmithing is needed to pull off a job, reviewing the findings of the job walk get them out in the open as soon as possible.

### **Quiz**

Finally, after reading, [take our 5 question quiz.](#)

## Hazardous & Explosion Proof

Controlling access to hazardous environments requires equipment meeting specific ratings that certify they will not start fires or will not introduce potential contamination risks.



Understanding those ratings mandate careful selection. We explain:

- Where is explosion-proof access equipment required?
- What are the three considerations for Hazardous rated access control?
- Hazardous rated access equipment including Assa, HID, Interlogix, and others.
- Typical product cost
- What are the ratings? Including NFPA 70, EX, Division 1, Division 2, and ATEX directives 95/137
- What do the ratings mean?

### Explosion Proof Surveillance

For a companion piece detailing explosion-proof camera systems, and the specific requirements of that equipment see our [Hazardous & Explosion Proof Video Surveillance](#) note.

## **Where is Explosion Proof Access Equipment Required?**

In general, any location where ignition of fumes, vapors, or any flammable material is kept or processed may fall under a 'hazardous area' restriction. In general, fire potential is the concern, as locations with high radiation risk or toxic material exposures are less common and classified differently.

Examples of common hazardous area locations are petroleum-based chemical storage areas, like gasoline tank farms, chemical processing, and refining sites, or any locations where airborne dust may be ignited common to manufacturing plants or agricultural storage granaries.

Automobile fueling stations are not typically classified as 'hazardous areas' requiring special equipment, however, care should be taken to confirm or investigate if a location requires rated access control equipment.

### **Three Basic Considerations**

Access controlled openings, unlike video surveillance cameras, typically require multiple components all installed together within dangerous areas. Therefore, all hazardous area access needs to be installed observing three basic rules:

1. All devices located in the hazardous area, like readers and locks, need to meet explosion-proof ratings of the area.
2. Any data or power cabling for those devices need to be made intrinsically safe when it enters the area.
3. Wiring connections to devices like readers and locks should not be capable of causing a fire.

These requirements generally can be accomplished by using rated equipment with the approval of an AHJ. Options for meeting specific ratings can be readily found, as we detail in the next section.

## What equipment satisfies this requirement?

In general, access control inside hazardous areas locates as many system devices as possible outside of the rated area. Accordingly, components like access controllers, panels, low-voltage power supplies, and network switches are installed in safe zones and require no special ratings.

However, not all devices can be moved and must be hung immediately adjacent or onto openings within a hazardous area. The most typical components needing to be certified are detailed below:

### Readers

Because credential readers and keypads are typically hung immediately at the opening, it is common that these devices must carry a rating.



A number of options exist that depend on specific rating and credential format support but include examples from large manufacturers including:

- [HID Global/Class 1 Div 2 Mullion \(~\\$300\)](#)
- [Honeywell Class 1 Div 2 Keypad/Gate Interface \(~\\$1,200\)](#)
- [Sentry/ Class 1 Div 1 Enclosure Mount \(~\\$800\)](#)

### Door Position Switches and RTE Devices

Another device typically hung onto doors in hazardous areas is [Request to Exit](#) devices and [door position switches and contacts](#).



Rated examples include:

- [Assa Explosion-proof RTE Pushbuttons \(~\\$1,100\)](#)
- [Interlogix Magnetic Contact \(~\\$125\)](#)
- [Falcon EX Rated PIR \(~\\$900\)](#)

## Locks

Interestingly, maglocks are the most common type of hazardous rated lock available, despite other types of locks like [electric strikes](#) being preferred for traditional openings. Maglocks are used because their typically potted, solid-state, and enclosed construction is easier and less costly to manufacture as explosion-proof compared to the basic inductive coil/solenoid driven operation of strikes and exit devices.

However, special order products from manufacturers like [Securitron](#) are available.

## Integral Door Locks

In many cases, the explosion rated door or gate itself will be designed with a mechanical security lock, and the access system will integrate to it via controller or relay contacts. However, other elements of the door may be responsible for keeping a door closed, or even open, as in

the case of explosion rated [Door Holders](#) and [Door Operators](#). These devices are application and opening driven and may cost \$5,000 or more.



### Airlocks/Mantraps

In many cases, aggressive forms of controlling access are physical elements of opening design for hazardous areas. Features like door [interlocking systems](#) or elevator interlocks designed to allow only strictly controlled and verified personnel into the rated room.

As we note in our [Mantraps](#) note, these features typically involve using a series of doors and separate rooms to segregate hazardous areas from general populations of people.

### Explosion Proof Enclosures

In some cases, non-rated equipment must be installed in hazardous areas, and elements like cabling or power wire must be run into a rated area.



For this, a variety of general-purpose enclosures, junction boxes, and wire seal compound is available. However, the rating and degree of protection needed from these general items are subject to [AHJ](#) approvals:

- [Rated Enclosures](#)
- [Wire Termination Seal Compound](#)
- [Rated Junction Boxes](#)

Prices for these general items can range from a few hundred to thousands or more dollars depending on dimension, rating, and whether or not being filled with inert gas or sand is required.

### **Explosion Proof vs Blast Resistant**

For openings, two different rating systems are often cited as 'special conditions' and may even appear together in the same door. However, these ratings indicate two distinct properties:

- **Explosion Proof:** Doors and related equipment will not introduce or sustain potential ignition in a hazardous environment
- **Blast Resistant:** Doors can sustain an explosion or pressure load and still retain their structural properties

It is important to not confuse these requirements and assume either preserves proper ratings.

### **How do I know when to consider special rated equipment?**

If you are an integrator, security manager, IT manager or manufacturer, you should not be deciding whether or not special rated equipment is required.

Typically, the '[AHJ](#)', or 'authority having jurisdiction' makes this determination. The AHJ might be a Fire Marshal, an operational risk assessment engineer, occupational safety authority, or even an insurance underwriter. That individual will classify the hazardous area based on risk criteria. It is the best interest of the owner/operator of such an environment to realize, control, and mitigate any potential risks in the hazardous area – including the installation of electronics equipment like surveillance cameras. Installers are typically asked to provide appropriate certification of the furnished equipment.

In general, a key indication that hazardous access gear is required comes from observing occupational protective equipment or process equipment in the area. For example, if all area workers need to wear electrical grounded clothing or if area fork trucks have an EX rating, the area likely requires explosion-proof access equipment. However, it is important to base equipment specifications upon solid confirmation of the area, as the cost of equipment certified as 'safe for use', or 'intrinsically safe', is significantly more expensive than non-certified equipment.

### **What does a particular 'hazard rating' mean?**

Worldwide, a variety of hazardous area certification marks exist, and it is appropriate to furnish equipment that satisfies whichever prevailing standard applies to your application.

### *United States*

In the US, [the widely adopted "National Electrical Code](#) or 'NFPA 70', defines environments by flammable volatility. The classification is segmented in three (3) classes, with a Class 1 environment being the most volatile typically including sites that handle gasoline and chemicals. An accompanying clarifier (the Division) denotes the default danger 'type of condition', being Division 1 – normal, or Division 2 – abnormal.

In this manner, the risk of fire or explosion in a hazardous location can be qualified. For example, portions of a fuel transfer facility may be designated as a 'Class1/Division1' area, while a wood pulp storage facility may be designated as a 'Class3/Division2' facility. Both classifications denote some risk, but certainly, the risk is qualified as being more significant in the area with the lower rating.

### *Globally*

In the EU, a rough equivalent for the NEC's Class/Division rating is noted by the 'ATEX directives, 95/137'. While technical definitions of hazardous areas differ (and may not overlap) among standards, the ATEX directive seeks to quantify hazardous areas in the same manner.

In South America, especially Brazil, the INMETRO risk classification system performs the same function as the bodies listed above.

While independent of each other, these ratings all seek to explicitly define hazardous areas.

## "Future-Proofing"

It's one of the most misused phrases around: "Future-proof". However, even without the crystal ball and wizards, designing access control to be "future proof" is much more practical than the concept implies.

The features we tag as 'future proof' are:

- OSDP
- Smartcard Frequencies
- Door Controllers
- Third Party Controllers

While we explain why these products or features should be avoided:

- ONVIF C
- 125 kHz Cards
- Combo Readers and Controllers
- Mobile Credentials

We explain the pros or cons of each technology and how following these guidelines can save you thousands or more.

In the sections below, we describe the access technologies to adopt and avoid for the best results for years to come.

### Adopt

First, here are the technologies to use in your access system, and why you should:

- *OSDP*: A new approach that resolves longstanding security vulnerabilities between controllers and readers is OSDP. The protocol is billed as a replacement for Wiegand by offering advantages like encryption, two-way communication, and accommodates more credential data, faster. (For more detail, see our [Wiegand vs OSDP](#) note) Moreover, while the protocol is still new, adoption by industry majors has been widespread with leading companies on both the reader and controllers side already adopting it.
- *13.56 MHz Credentials*: While not new, the market has been slow to migrate to the higher frequency, more secure 'smartcard' frequency format. However, as time progresses, the availability of older formats becomes more difficult and expensive [link no longer available], security risks aside. With mainstream vendors like [HID building new readers](#) that primarily use 13.56 MHz formats, avoiding costly changeovers mean adopting the format now.
- *Decentralized Controllers*: In the past, the most common architecture for access was to use one panel to control four or more doors, sometimes as many as [32 in one enclosure](#) or even eliminating door controllers entirely (see our [Eliminating Control Panels? Viscount](#) review for one example). However, with the emphasis and availability of IP networks within modern facilities, adding a 'smart controller' at the edge is not a challenge and offers savings to endusers in reducing cable and installation labor to a few feet rather than homerun to central closets.
- *3rd Party Hardware*: While 'proprietary' cannot be eliminated outright from access, restrictions can be lessened by adopting hardware controllers that can be used in multiple systems. Options for interoperable devices are limited to the three major providers and controllers we list in our [Axis vs HID vs Mercury Access Controllers](#) note. An enduser with hardware from one of these providers typically has multiple management platform options to chose from if the current choice is failing to get the job done or goes out of business.

## Avoid

And here are the technologies to steer clear of and the reasons why:

- *ONVIF Profile C*: Despite grabbing attention early, ONVIF's access interoperability guideline has fizzled with no significant adoptions since Axis released their A1001 two years ago. The current outlook for ONVIF and other interoperability standards is grim with little market traction, detailed in our [Access Interoperability: Going Nowhere](#) note.
- *125 kHz Credentials*: Steer clear of older, much exploited, unencrypted contactless credentials using the 125 kHz frequency. Despite YouTube being full of videos revealing how to use \$50 cloning kits widely available online, many endusers and integrators still are adopting it is the key to their systems. In our most recent [Favorite Access Control Credentials](#) survey, a whopping 36% still call the type their preferred option. However, with costs for 125 kHz cards and readers typically equal or more than 13.56 MHz products, there is little reason to continue using them.
- *Combo Controllers*: While decentralized controllers make good sense, the idea can be taken too far, as is frequently the case by combining the controller with the reader. The major weakness of the approach is the vulnerability when hanging the units on the unsecured side of the door leaving the opening - and subsequent area security - at great risk to intrusion threats. We detail the risk in our [Access Control: Combo Reader / Controllers Tutorial](#) note.
- *Mobile Based Credentials*: Few access technologies have gotten the hype of smartphone credentials. The slick imagery of access users waving their smartphones in front of a reader instead of a stale, boring ID card may make for great tradeshow buzz, but shifting to mobile is expensive and raises big operational problems, like how willing smartphone users will be letting employers manage device settings, how credentials are provisioned, and whether or not users need to carry cards anyway for picture IDs. We examine these major issues in our [NFC: Not Ready for Primetime](#) note, but they also apply to [BLE \(Bluetooth Low Energy\) for Access](#) as well.

## Cost Savings

The exact dollar figure impact of these decisions is substantial, and savvy designers and end users can save thousands by 'buying right' upfront.

For example, a 'forklift upgrade' of proprietary controllers instead of reusing existing 3rd Party Hardware can amount to over \$1000 per door when costing the additional controllers and installation labor. The cost of upgrading a reader to work with 13.56 MHz smartcards can be \$200 per reader and \$10 per card for each user when existing 125 kHz options are discontinued by the vendor [link no longer available].