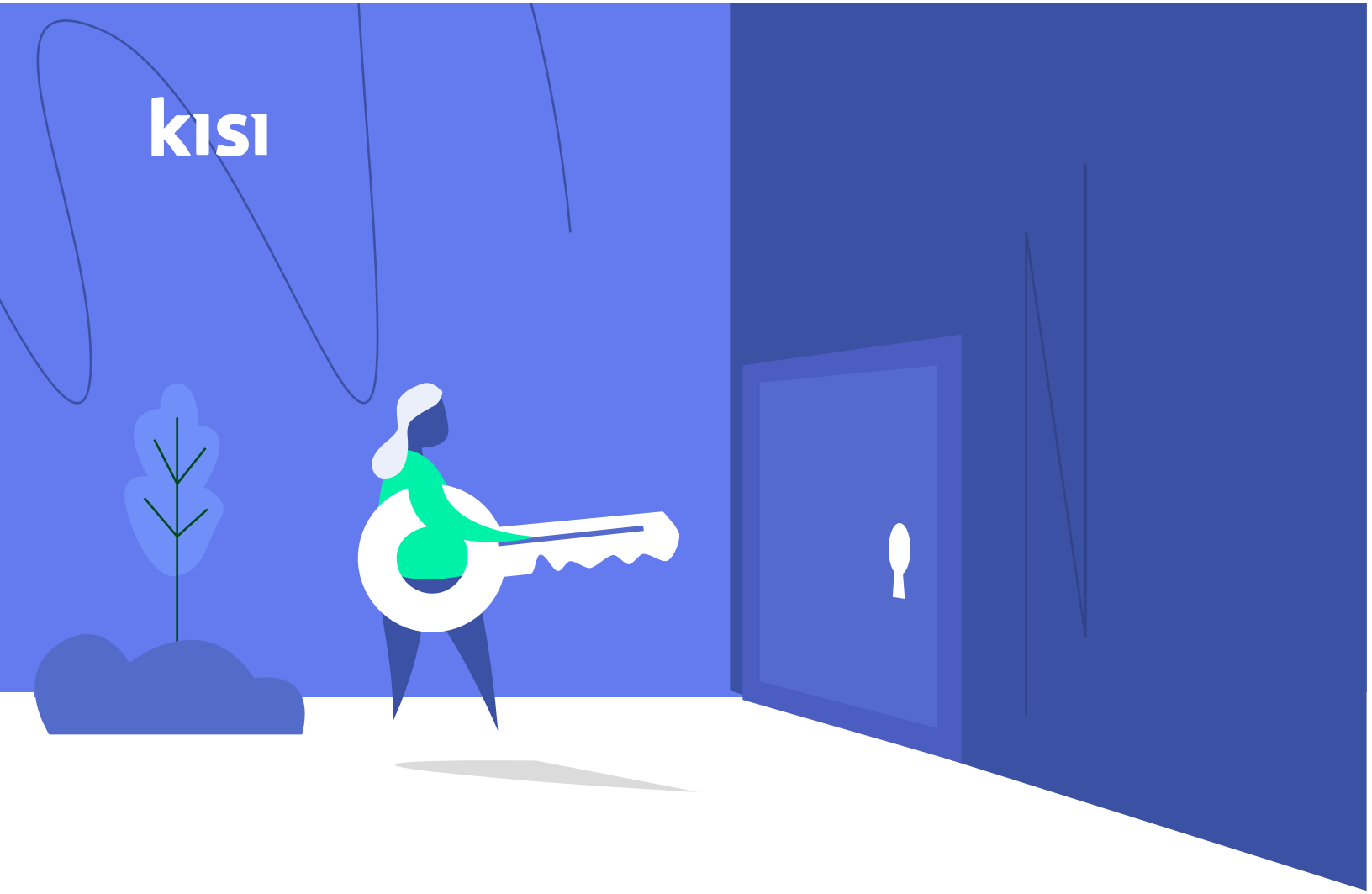
kisi

Introduction to Access Control Systems

A guide to getting started with access control

www.getkisi.com



Access Control Systems

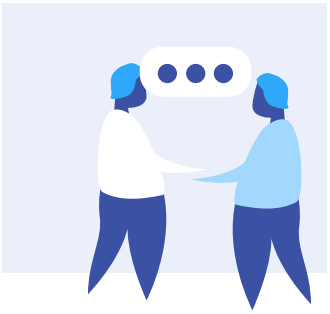
Getting started with access control can be overwhelming at first with so many technical terms and things to wrap your head around. But understanding access control systems is really an achievable goal - especially after reading this guide.

This is really a 101 crash course guide for access control systems. If you want to get a relatively quick idea of how access control works, you've come to the right place.

If you are new to the world of physical access control, you might have some questions like:

Components

What are the pieces of an access control system and how does it work?



Why

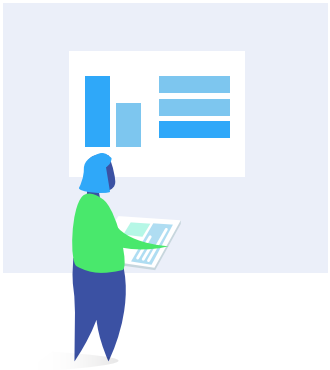
What are typical reasons why people choose access control?

Quote and Cost

How much should I spend on an access control system and how does a sample quote look like?

Setup and Operation

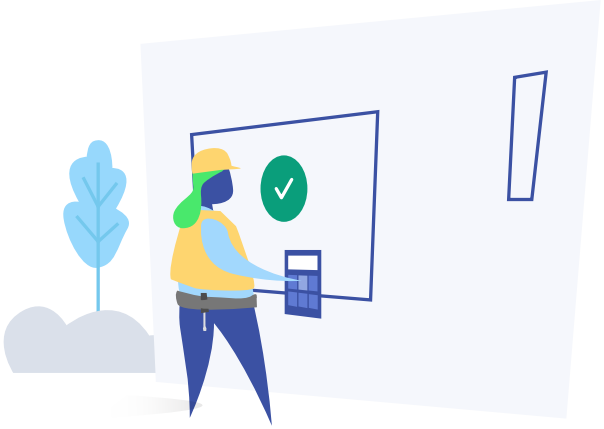
How do I set up a working access control system and where do I start?



Managing and Using

Who uses an access control system in day to day life?

All of these questions will be addressed in this post including links which contain detailed information for further reading. We've compiled a list with the 30 best security magazines and publications so you can get some information as to what is going on in the security market.



Here is an overview of how to find the best security consultant and what to look for

Free vs. Security Consultant

When looking at ways to learn fast about security, most people call a local security integrator, installer or security consultant. However understanding some basic things about access control systems is really easy when you have resources like this.

Is it absolutely needed that you learn about access control yourself? No, definitely not. However it will save you tons of time when you are into your project allow you to understand some of the basic terms commonly used in access control

Introduction to Access Control Systems

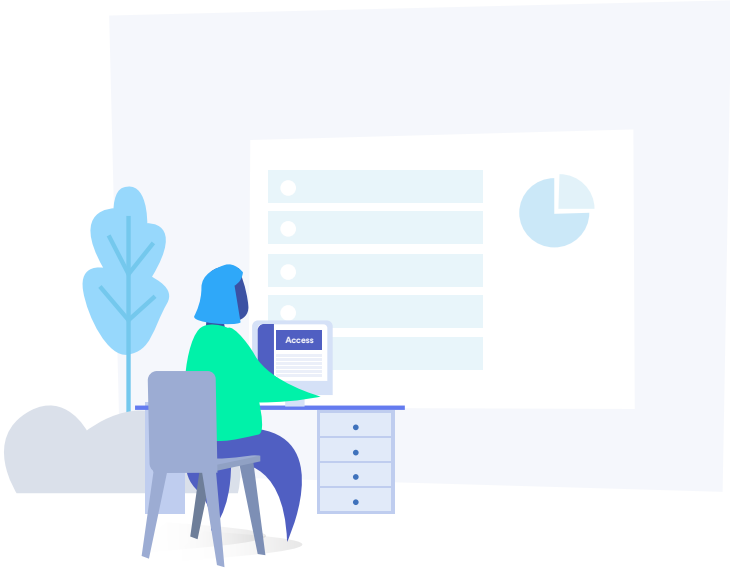
As long as you are carrying an access card or ID badge, it means that your office uses an access system
But how does it really work? It's difficult since most people have never seen an access system. Most people believe it is just a **card reader** on the wall.

Of course there is a little bit more to it in reality. It’s not very difficult though, there are just a few parts behind the scenes that make the magic of easily unlocking a **door** every time.

Reading this will give you a full and comprehensive understanding how access control systems work and the language needed to communicate about it with vendors.

What is an access control system?

Let’s keep this simple: An access control system allows you to manage, monitor and maintain who has access to for example your doors. The simplest form of "access control system" is a standard deadbolt with a brass key.



Since the introduction of the key some 4000 years ago, much more advanced systems have been introduced. Today there are different computer-based, electronic access control system types which we described in an earlier post.

Using an access control system allows you to manage access or entry to almost anything: file access, workstation access, printer access and in our case, door, facility, building or office access. The standard form of today’s access control is an “**access card**” instead of the key to grant access to the secured area. In the case of access to larger buildings, the exterior door access is managed by the building while the interior door - or tenant door access is managed by the individual tenant company.

Why do we need access control?

The purpose of access control is to provide quick, convenient access control for authorized persons, while at the same time, restricting access for unauthorized people.
Here are more reasons why access control is playing a significant role in your organization:

Compliance

Some companies need to be compliant with health data regulations **(HIPAA)** or credit card data regulations **(PCI)** or even with cyber standards such as **SOC2**.being able to pull compliance reports for access control can be a big request.

Experience

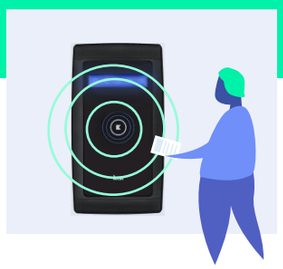
If you have a lot of visitors or clients coming in your space, you might be looking for a welcoming experience at the front door or front desk. Access control can not only help but also make your space better!

IP / Data

If you are working in a company with an expensive product or sensitive data. You definitely want to to control who is coming in your facility.

Basic Components of Access Control systems

Access control systems vary widely in type and complexity. However, most card access control systems consist of at least the following basic components:



User-facing

Access cards, card reader and access control keypad

Admin-facing

Access management dashboard, integrations or API

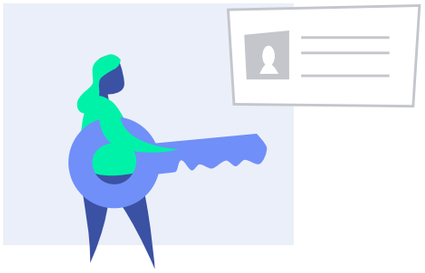
Infrastructure

Electric door lock hardware, access control panels, access control server computer and low voltage cabling

User-facing side of Access Control

The user facing side - often called “credentials” Access credentials in form of access cards, ID badges or smartphone based mobile credentials

When presented at a card reader on the wall, it beeps and hopefully you are permitted to access and the door unlocks. The user facing side is what you have on you that gets you the permission. The device on the wall reads your credential or permission. Here an example how that can look with a smartphone as access credential:



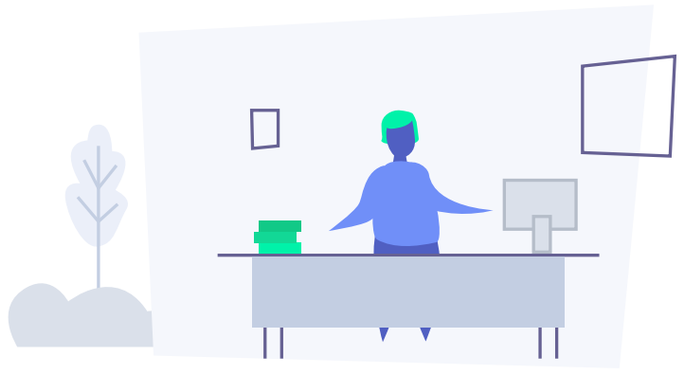
Credentials

This is your electronic “key” and what you have that gets you access. It could be access cards, ID badges, ID cards or smartphone based mobile app access. People can use it to gain access through the doors secured by access control systems. The form factor of access cards is the same as credit cards, so it fits in the wallet or purse. However demagnetization is very common with basic access control cards. The benefit of using credentials is that they are personalized, so **any unlock event can be tracked back to the person associated with the credential.**

Card reader

Mounted on the wall, the card reader electronically reads your credentials and **sends the request to unlock the door with your user credentials to a server.** Typically the type of cards used are proximity cards which require the card to be held in a **2” to 6” proximity** to the reader .
Card readers are mounted outside of the perimeter (exterior non-secured wall) next to the door they should be unlocking. In addition to card readers, some access control systems provide the option of using keypads (PINS) or biometrics instead of cards or smartphones as credentials. This is rather uncommon, since PINs can easily be passed on and biometrics are harder to manage.

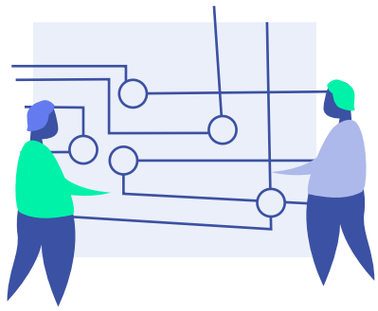
Admin-facing side of Access Control



The admin facing side is where your office **administrator, head of security or IT manager sets the parameters of who is allowed to access under which circumstances.** This involves a **management dashboard** (often in the **cloud** these days) and a way to provision access, e.g. a card programming device.

In more advanced systems the **manual operations aspect can be automated** - as an example the provisioning and de-provsioining (creating and deleting access) can be done automatically by connecting the access dashboard to your company directory of employees. When a new employee shows up in the system, a new access right is automatically provisioned via a directory like Google Apps, Microsoft Azure, SAML or Okta.

Management dashboard or portal where administrators can manage

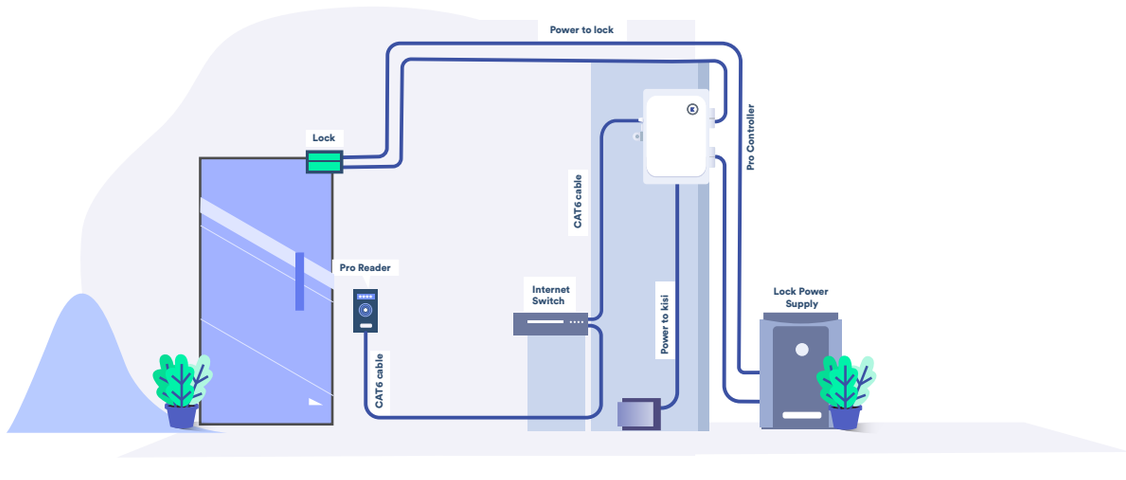


API and **integrations** can be used to automate manual workflows and make operations less prone to errors

Access Control Infrastructure

Access Ccontrol infrastructure is to most people the most mysterious aspect of access control systems. Obviously there are **electronic locks** installed - but what most people don't know: Those locks are all centrally wired to your IT room. This means: **A power or signal cable** runs from the lock through the walls into your IT room where the access control panel sits. The access control panel gives the lock the signal to unlock when it receives the request to do so by the card reader. There are different topologies (as people call it) but for the basic understanding of access control systems let's just assume this described flow for now.

An overview of Kisi's wiring diagram of a basic access control setup:



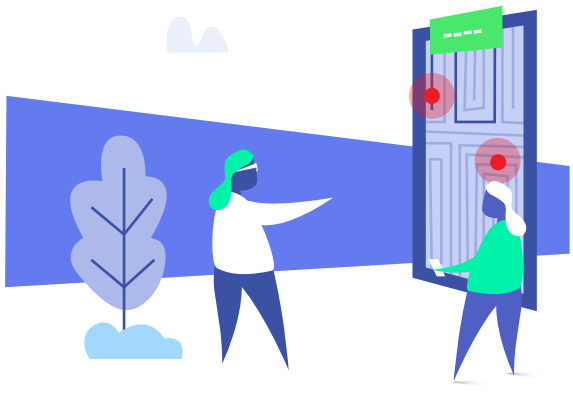
Locks

Electronic locks are used to electrically unlock the door that it is installed on. They typically have a wire that supplies them with power.

Some locks open when power is supplied (**fail secure** locks) and some locks lock when power is supplied (**fail safe** locks). The reason for those two types of locks is the following: In the event of fire some doors like your front door should open to comply with building and fire codes to allow people to exit the building facility at any time. Other doors like an IT room door are wired **fail secure** and should remain locked even during an emergency.

In terms of the electronic locks used, we see everything from electronic strikes, electromagnetic locks (mag locks), electric exit devices, electrified mortise door lock sets and many more. Based on your door type and construction, the integrator will specify the best lock to install.

Independent of the lock installed, they are typically wired back to the access control system panel.



Access Control Panel

The access control panel is not visible for most people in a facility since the access control panel (sometimes called "access control field panel" or "intelligent controller") is installed in the IT room, electrical , telephone or communications closet (comms room). The reason why it is behind locked doors is because all locks are wired to the access control panel. When a valid card is presented at the card reader, the **door access panel receives the request to unlock a specific relay which is connected to a specific door wire. When the relay triggers, the lock is being powered** (in the case of fail secure locks) **and the door unlocks**. This is how the **access control panel** control the access activity for building doors. How many access control panels have to be provided depends on the number of doors each panel can control. Kisi's access control panel can control up to 4 doors. If there are more, they can be modularly added next to each other.

Access Control Server

Every access control system needs a server where the **permissions are stored in an access database**. As such it acts as the center or "brain" of the access control system. It is really the server which makes the decision if the doors should unlock or not by matching the presented credential to the credentials authorized for this door. The server can be a local windows or linux server, a cloud server or even a decentralized server when credentials are stored in the door reader.The server also **tracks and records activity** and events regarding access and allows to **pull reports of past data** events for a given period of time.If a local hosted access control server computer is used, it is typically a dedicated machine that runs the access software on it. This is the reason why **cloud based systems** recently gained a lot of traction since multi-facility management can become complicated with local servers.

Low Voltage Cables

Often overlooked but sometimes actually the most expensive part of an access control system when done wrong. When building out the space it is important that **all the necessary cables are specified**, so the general contractor knows what to do. If the **cables** are not planned in at this point, they need to be added later and someone will have to drill in that newly painted wall or run cables on top of your beautiful walls.

A simple access control system quote example

Lets say you have an office or building with **two doors** that are on opposite ends of the facility, like a front and back door.

Currently in use are regular keys to unlock and lock the door. The Management is looking to improve security and operations on this facility by implementing an access control system. Reasons for looking into access control systems because your company is growing and you'd like to have more control.

After taking a closer look at the doors that are security sensitive, the **IT room door** came to mind since there are many security related devices and equipment installed. The **door leading from the hallway to the IT room** should be secured as well.

A team member is typically tasked with researching different access control options and getting bids. The team member is researching a few local vendors to contact who supply and install access control. Typically they will stop by to take a look at your space and the doors to give you an accurate quote for the access control system. Here is a sample of how a one door access control system quote look like:

[redacted]

QUOTE

DATE	INVOICE #	CUST #
11/9/2015	0000025032	0000287

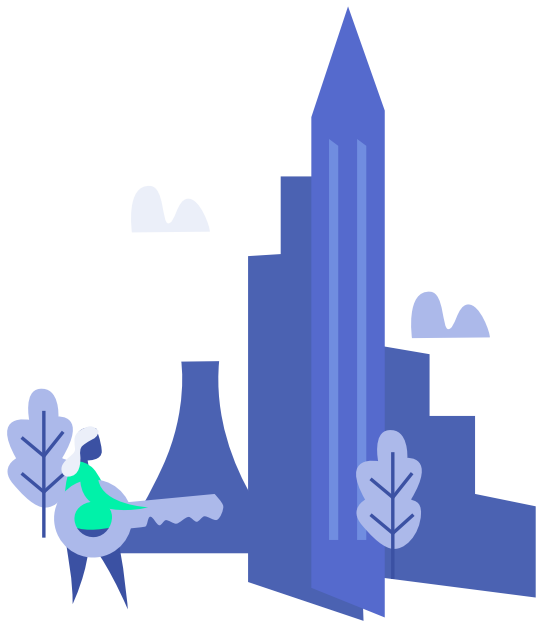
SHIP TO: [redacted]

P.O. NUMBER	TERMS	SALES PERSON
	NET 30	[redacted]

QUAN	DESCRIPTION	PRICE EACH	AMOUNT
	Total Materials		1,856.28
	Total Labor		1,468.17
	[redacted] Fees are INCLUDED for the first twelve (12) months and are collected annually in advance. Cancellation of [redacted] service requires 30-days minimum notice (after initial 12-months). Billing period begins on the 1st of each calendar month.		
	[redacted] Fees for one (1) door will renew at the (Current) rate of $14 per month and are collected annually in advance.		
	Provide and install a 1-Door [redacted] Access Control System to allow access using the Building-issued cards as well as the tenant-provided cards/fobs or mobile devices. Complete turn-key solution is provided, including the electric strike and replacement mechanical lockset on door.		
	Optional [redacted] MobilePass - allows unlocking of door using the [redacted] mobile app on mobile devices (does NOT require a card/fob). This is an add-on feature that starts at $19 per month for 100 mobile passes. Mobile passes can be revoked and reissued at any time. Account comes standard with five (5) mobile passes that can be used for no additioanl cost		
	SUBTOTAL		$3,324.45
	TAX		$175.55
	TOTAL		$3,500.00

Sample access control quote

(Many installers pack a lot of information into the quote and **not necessarily provide line items**. There are many ways to understand vendor or installer quality and the quote certainly is one of them)
Going back to our example: The integration vendor conducts the site survey and determines that in this case there are **three card readers needed**. For the locks installation of two magnetic locks on the glass doors and one electric strike for the IT room door is suggested. installation of an access control panel is recommended by the installer which connects the door locks to the internet.



Also included is the wiring to connect everything and set up the system, a license for maintenance and support which sometimes includes the hosting and a few accessories. Vendors sometimes include a trip charge or service call.

Because the company **wants to manage access from remote, a cloud-based physical access control system is recommended**. This allows logging on to a web based portal from any browser and - given the correct credentials are presented - to make changes to the access rights and share or revoke access from remote.

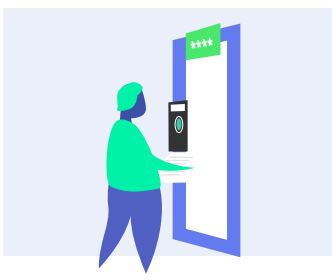
Again, the most important thing about quotes is that you **get line items so you understand what is being done.** If the access control installer lumps everything together in one sum like above they sometimes ballpark the numbers and don't specify the brand of hardware they use
It is of high importance to clarify at this point if the quote includes a **Certificate of Insurance (COI)** which you can ask your building management if you are required to have this for incoming vendors. This makes sure possible damages by a vendor up to a certain amount are covered.

Access Control System Setup and Operation

Once you found the access control system you like, what happens next? How does the system get installed in your space?
Here is the answer: Typically installers take a few days from confirmation of the order till actual installation because they need to order the parts needed for the installation. Once you have an actual installation date, you'll find that the installer will do the following:

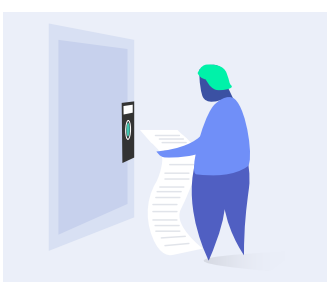
Run the cables

If you don't run the cables you can't connect anything, so it really makes sense to start with running the internet, power and signal cables first.



Install the readers at the door

Mostly the just have to be screwed on the wall and connected to power. Some readers like the Kisi IP reader need internet connection and would have to be connected to the internet.



Setup and testing

If there is a server to set up, it's typically done after everything is installed so the software can be configured and tested if all doors unlock correctly.

Install the access control panel in your IT room

If you have two doors, you will be able to live with one access control panel because most of them can handle multiple doors. The integrator might install a backup power supply or other additional security hardware depending on your building's specifications.

Install the locks

Depending on what type of door you have, the integrator will either install a magnetic lock, electric strike or electrified mortise lock. This might involve cutting into the door-frame which is why sometimes it makes sense to do first so the office workers are not annoyed in the middle of the day

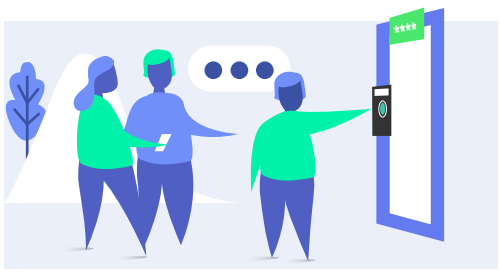
Using the Access Control System

Once you have the door access system set up - you might run through the following steps to roll out the access control to your organization:

Set up a door access schedule

When should some doors unlock, when should they be able to accessible in general and which types of access groups or individuals should be able to gain access. Are IT managers are allowed to access all doors? What about executives? Are they allowed in the office 24/7? It's a good exercise to discuss this with your security, facilities and management team as these rules is what your entire access control strategy will be based on, i.e. it will **determine what you actually want to control.**

Because the company wants to manage access from remote, a cloud-based physical access control system is recommended. This allows logging on to a web based portal from any browser and - given the correct credentials are presented - to make changes to the access rights and share or revoke access from remote.

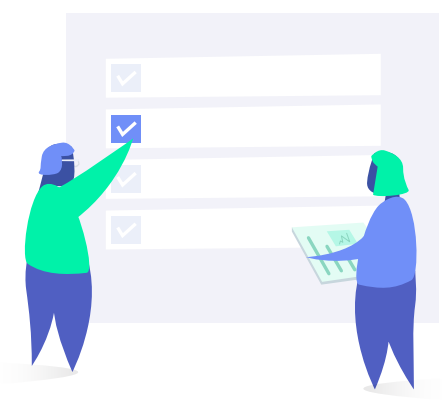


Test the system with a few pilot candidates or coworkers

Try running through the process that you envision for every employee or visitor. Provision access for them, activate their access, hand over the access card or share access with them, then see if it works for them. If you roll out too quickly your process might have some smaller hiccups and the more people you involve, the faster the problem multiplies.

Set up the rules in your access control software and test if they work

Under certain conditions you want the user not to be able to unlock the door and so on.
Pro tip: Many offices get broken into during vacation days. Some offices automatically unlock their doors during work days. If the work day is a public holiday, burglars know they might just be able to walk in.

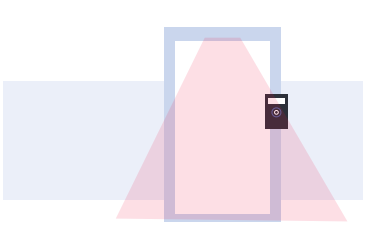


Announce the roll-out

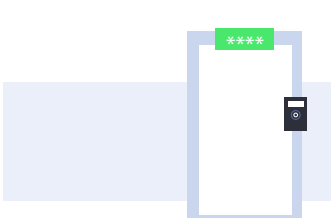
Send an email to everyone to **announce the change in access control**. People don't like change - some might have an emotional bond to their physical key, so make sure to be ready for pushback and highlight why this makes your workplace safer and your company more secure in general. Everyone should be able to agree to this.

Onboard your team

Once the system is tested, announced and approved the fun part begins: The actual roll out. You can start provisioning access for your team. The most important to consider is that some people will have issues or problems getting access, so make sure to **roll out on a day that is not the most critical** - most people choose fridays so there is time to troubleshoot.



Door Status Monitoring Feature



Automatic Unlock Feature

Reporting Feature

Check out Kisi's product pages for more advanced features:

- Kisi Access Reader
- Kisi Cloud Access Dashboard
- Kisi IP Control Panel
- Kisi Mobile Credentials.

Discover Kisi in action

We provide an **easy-to-manage**, scalable system to regulate security for businesses of all sizes.. The best access control systems **combine** top-notch software with the right hardware

How it Works

Flexible Pricing & Quotes

Get a tailored quote that fits your business location and needs. All paid plans come with a 30-day trial window and we also ship and install with remarkable speed

View Pricing Plans

We would love to hear from you

Get in touch with our sales team with a brief summary of your needs and we would get back to you within one business day

Contact Us

CALL US

646-663-4880

EMAIL

sales@getkisi.com