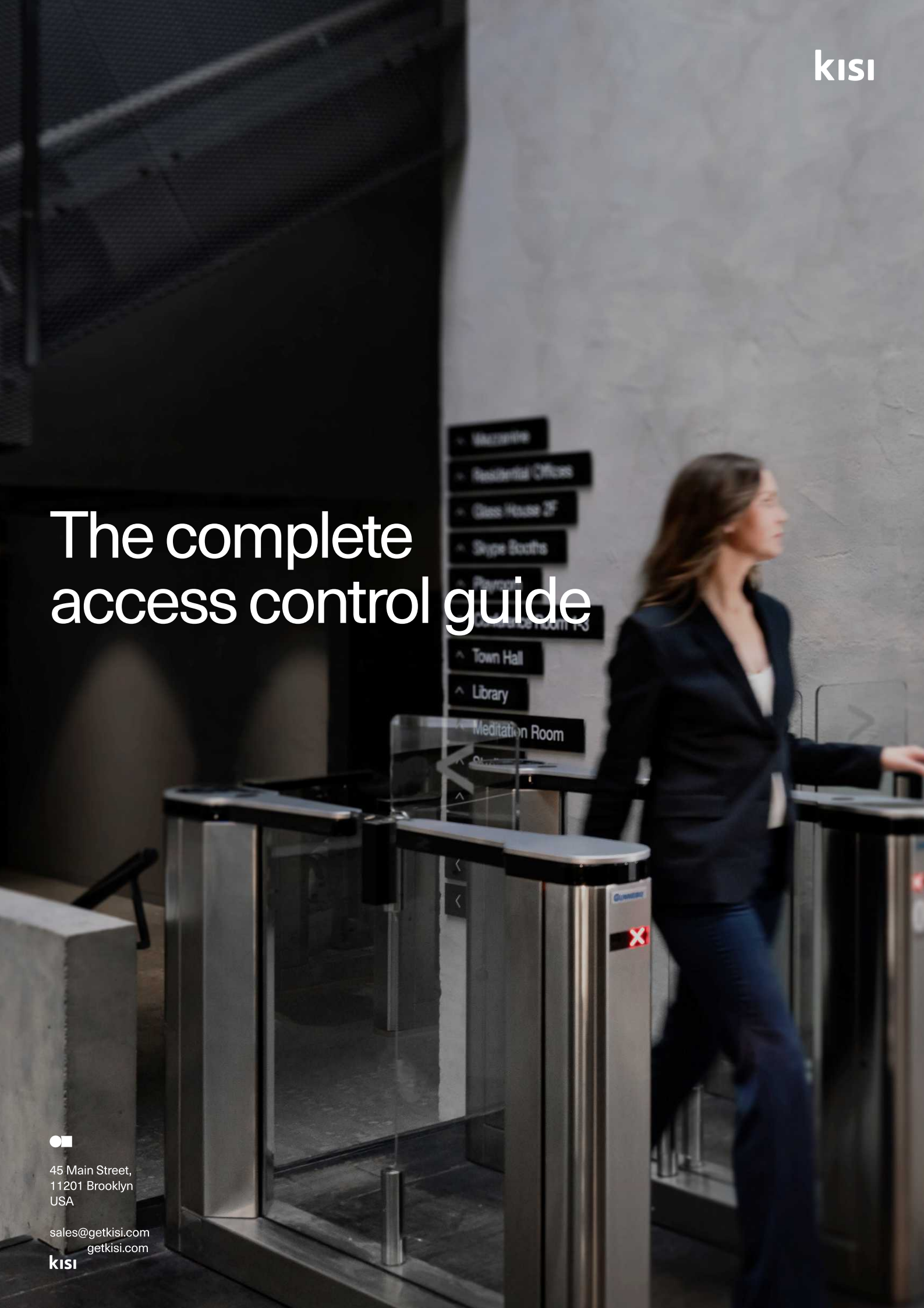
kisi

The complete access control guide



45 Main Street,
11201 Brooklyn
USA

sales@getkisi.com
getkisi.com

kisi

Table of contents

Introduction

Access control is one of the most crucial aspects of any company's security.

A weak access policy that regulates the flow of employees and visitors entering and exiting your facility might lead to breaches and compromise your company's physical and digital security.

Use this guide to explore the access control components, use cases, and integrations to build the ideal setup and enhance the security of your business.

Discover the tools to make the best decisions and clear up any doubts regarding hardware and the technology behind the scenes.

What is physical access control?

The purpose of physical access control is to grant entrance to a building or office to only those authorized to be there. The deadbolt lock and matching brass key were the gold standard of access control for many years. Times are changing and modern businesses require more than simply controlling who passes through their doors. They need to monitor and manage access remotely, automate their security, and integrate access with the software they're using.

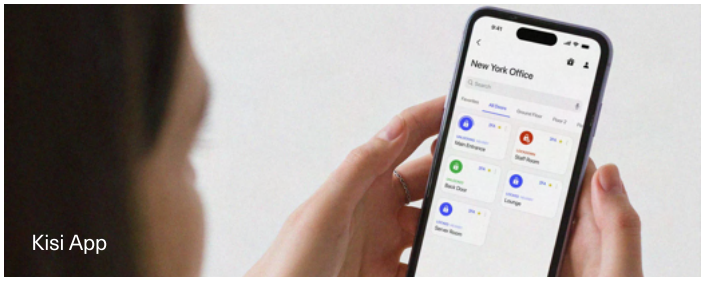
Keys have now passed the baton to cloud-based devices and systems that provide quick, convenient access to authorized people.

Today, instead of keys, we carry access cards, ID badges, or smartphones to gain entry to secured areas. Access control systems can also be used to restrict access to workstations, file rooms housing sensitive data, printers, and entry doors.

In larger buildings, the landlord or management agency usually manages the exterior door access, while the tenant company controls interior office door access. Cloud-based access systems like Kisi offer solutions to easily bridge this gap.

People new to access control may think the system consists of only the card and the card reader mounted on the wall next to the door. But there are a few more parts behind the scenes, all working together to make the magic that grants access to the right person happen. That's what this guide is about. Reading it will give you a comprehensive understanding of how access control systems work and how to choose and set up the right one for your needs.


Reader Pro 2



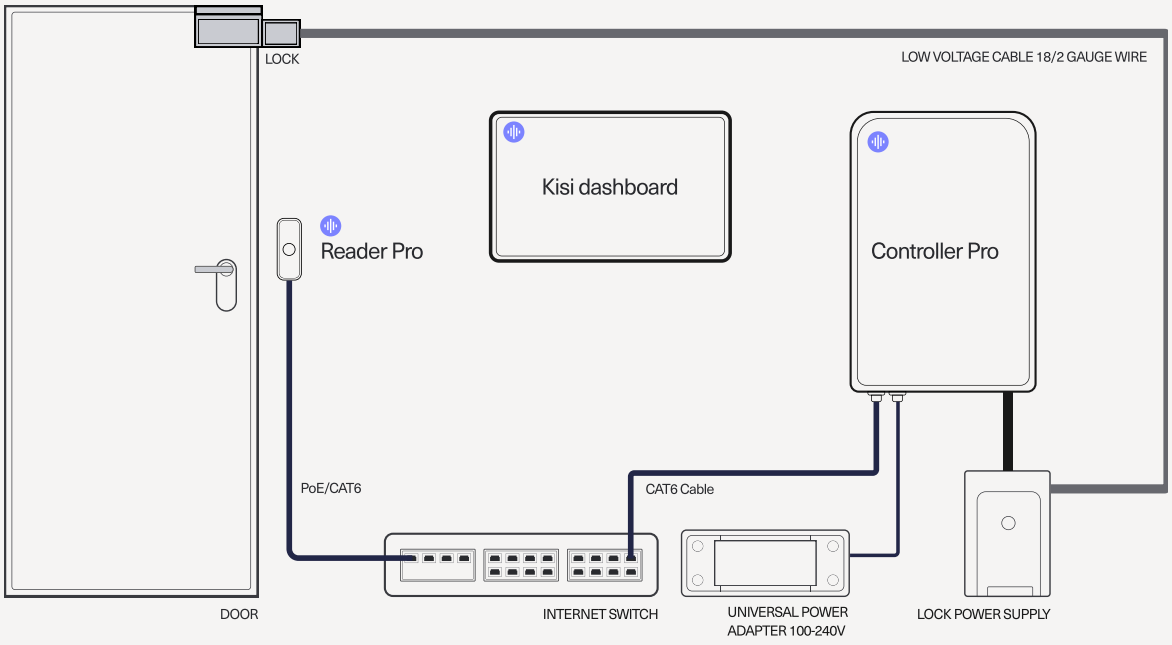
Kisi App


MotionSense


Badges in Apple Wallet

Physical access control system components

Access systems control who has access to a building, facility, or secured workspace area, like a server or printer room. Access admins enable this by assigning employees, executives, freelancers, and vendors to different types of groups or access levels. For example, they might decide that all employees use their access cards to enter the main door, but some may not be able to access areas containing secure or privileged information. For clarity, let's divide the components into three groups: user-facing, admin-facing, and infrastructure components.



User-facing access control components

Access readers

An access reader, also known as a card or proximity reader, is the electronic device mounted near the door that access control systems use to grant or deny access to secure areas. The reader interacts with the access panel and the other user-facing component – the access credentials, to verify the permissions of the person requesting access.

The reader uses various technologies, like Radio Frequency Identification (RFID) or Near Field Communication (NFC), to communicate with the credential and validate the credentials against a database of authorized users to determine if access should be granted or denied.

Advanced access readers, like the Kisi Reader Pro, support multi-factor authentication, integrate with other security systems, and enable different mobile access methods. They offer a convenient and seamless user experience and a secure platform for your business.

Modern access readers enhance security by allowing real-time connectivity and auditing capabilities. For instance, the Kisi Reader records, logs, and organizes all access data, enabling capacity management and intrusion detection.

»The Kisi Terminal Pro—More than a card reader«

Expanding the functionality of the Reader Pro into a versatile check-in station and QR code terminal, the Terminal Pro supports various credentials, including QR codes, Apple Passes, badges, and MotionSense. The QR codes provide a user-friendly experience and do not require an app download or internet connectivity. Furthermore, they mitigate the risk of remote unlocking, offering additional peace of mind for security-conscious organizations.

Access credentials

The most familiar parts of access control systems are the cards, ID badges, fobs, and smartphone apps that elicit an OK beep when presented at an access reader and unlock the door. These are also known as credentials since they hold the user's data that tells the reader to grant authorized access or not.

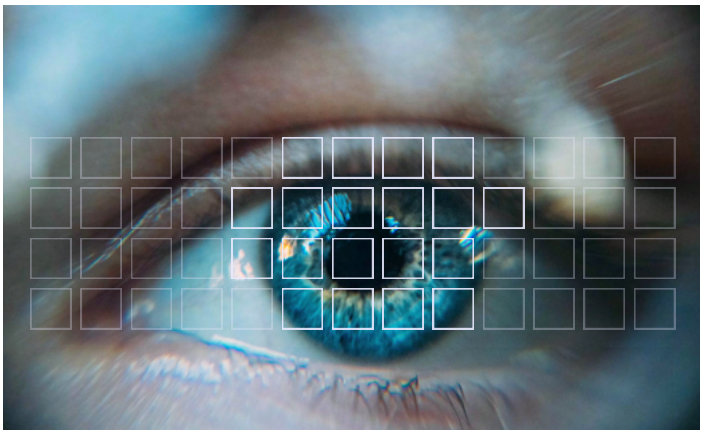
Access cards are typically proximity cards the user needs to hold two to six inches in front of the card reader. The same procedure is followed for phone apps. The biggest benefit of using credentials instead of the usual keys is that they are personalized, so any unlock event can be traced back to the person associated with it.

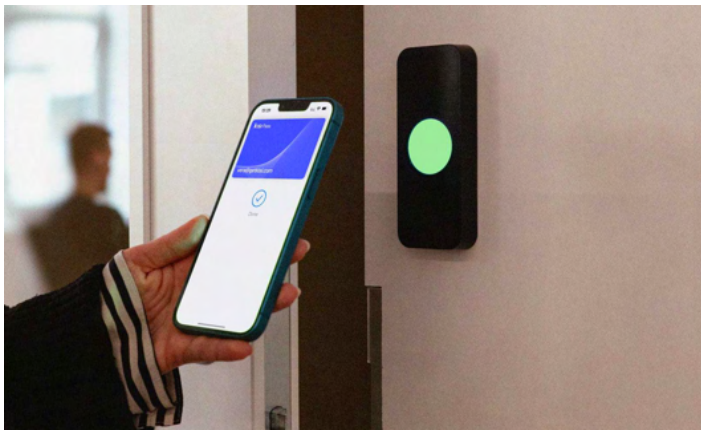
There are a few popular credentials options, so choosing the best one for your facility can be challenging. Explore the following table for the most common access methods, their ranking, and their ideal use case.

Access control methods assessment

CREDENTIAL	SECURE	CONVENIENT	SCALABLE	USE CASE
Physical keys	3	1	1	Unlikely to be a good solution for your business. Often employed in certain scenarios, like accessing low-security areas.
Keypads	5	8	1	Keypads are good solutions for sharing access with a small number of users, like in a residential setup.
Keycards	7	5	3	The level of security mostly depends on the keycards and systems used. Unlike phones, cards are more prone to be shared.
Fobs	7	5	3	Mobile unlocks made key fobs unnecessary. But in some environments it is still a good credential to provide users with.
App unlock	10	8	10	Unlocking from a phone is the most secure option given the additional biometric authentication method (fingerprint, facial recognition) most mobile devices encourage. Most scalable since it works even without a reader installed at the door.
Tap to unlock	9	9	10	One of the most convenient methods, as we all carry our phones on us anyway.
MotionSense	9	10	10	Mobile-based authentication combined with a motion trigger (usually moving the hand in front of the reader).
Badges in Apple Wallet	10	10	10	Similar to Tap to unlock with an added layer of security and reliability, like the advantage of unlocking doors even if your phone runs out of battery.
Access links	7	9	5	The level of security depends if best practices are observed. Access links are most suitable for allowing visitors or temporary staff to unlock doors.
QR codes	7	9	7	Most people are familiar with QR codes, so they're go-to options for visitor and member management in most cases. The level of security depends on how well the best practices are observed.
Biometrics (face recognition, fingerprints)	10	9	3	While mostly secure, biometric access presents several challenges, from privacy concerns to scalability limits.

Biometric access control





Biometrics have become quite popular in access control in recent years.

By biometrics, we mean the patterns in various body features (face, iris, fingerprints, or voice recognition) that are used in the context of access control to unlock doors or to authorize access to determined areas.
Biometrics is a controversial topic, as many still consider it a questionable way to authenticate. The criticism often revolves around how biometric data is stored. It is very difficult for a company to ensure that the data won't be used for other purposes that are not access-related, and for this reason, many employees refuse to even use these solutions in the first place.

Due to the nature of this technology, biometric authentication is hard to scale. Also, it doesn't work with visitors or users requiring temporary access, so its use case can only be limited to low-traffic environments.

The recent surge of biometrics in personal devices, like smartphones, empowered people to use this secure authentication method. Modern businesses utilize this development by implementing Kisi's mobile access control. This way, businesses get additional security with 2FA while users don't divulge their biometrics to the employer. With this method, Kisi users need to use biometric authentication on their mobile to unlock it before tapping the Kisi app or their phone against the reader to unlock the door.

»Employee badges in Apple Wallet«

Apple Passes resolve even the smallest questions some people have with mobile credentials. On the surface, offering a similar access method to tap-to-unlock, employee badges in Apple Wallet enable staff and guests to easily access their corporate spaces with just their iPhone or Apple Watch.

No need for a separate access control app, the ability to unlock doors up to five hours after your phone battery has run out, and taking full advantage of the privacy and security features built into iPhone and Apple Watch are some of the benefits offering additional security and convenience.

Admin-facing components

The admin-facing side is the access management dashboard or portal.

The users with admin permissions, like office administrator, head of security, or IT manager log in to the web or mobile dashboard and set the access permissions and schedules. This determines which individual or user groups are allowed to access the premises or specific secured areas and under which circumstances they can do so. Modern businesses prefer to work with cloud-based management dashboards for remote management and advanced functionalities.

In more advanced systems, like Kisi, manual operations, like issuing credentials, can be automated thanks to the vast integration options. For example, Kisi admins can automate provisioning (creating and deleting access) by connecting the access dashboard to the company directory of employees. When a new hire shows up in the system, new access is automatically provisioned via an API or integrating database service like Google Apps, Microsoft Azure, SAML, or Okta. Kisi is compatible with all major SSO providers and supports the SCIM 2.0 protocol.

Tom Parker
CISO | KAYAK

» I care so much about collaboration and experience. Everything I do, I take that into consideration. For me, Kisi is about being sure that we have the least impact on employee experience and support agility, innovation, and productivity. «

Read Case study

Kris Chaney
Director of Ministry Operations | Saint Jude Catholic Church and School

» It's the right complexity system. It does what we need it to do, but it doesn't have 12 dashboards and a hundred automatically generated reports, and it's not setting off alarms every time somebody scans in the door.

We can get the information we need, and the interface is very user-friendly. It's significantly more cost-effective than those more complicated systems, which is simply more than we need. «

Read Case study

Brandon Branham
CTO | Peachtree Corners

» Before Kisi, I needed the person to WhatsApp me and let someone in. Badges got lost on a daily basis. I needed remote access that would work for multiple tenants and support 24/7 access - as well as provide clean record tracking for audit purposes. «

Read Case study

Brandon Babcock
Building & Infrastructure Manager | Doctors of BC

» As a person managing the property and the building, being able to access doors and use them anywhere is phenomenal. «

Read Case study

Explore Kisi

Explore case studies Benefits of Kisi

Infrastructure components

The infrastructure components, like access panels, locks, and cables, are closely connected to the building infrastructure.

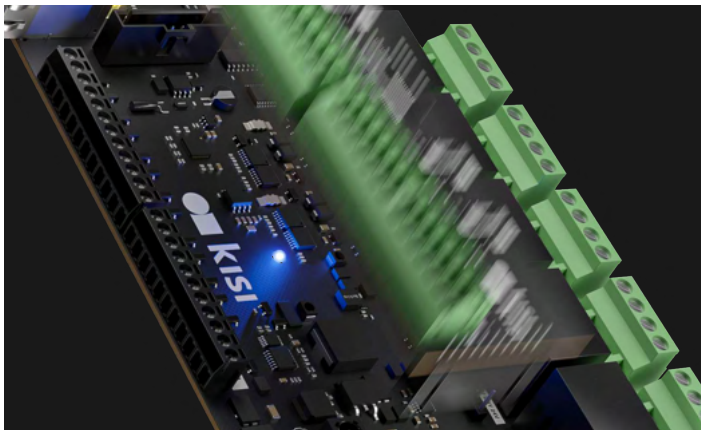
Access control locks

Electronic locks enable keyless entry, eliminating the need for physical keys. The ones for commercial use are usually wired to receive power. There are two types. Fail-safe locks lock, while fail-secure unlock when supplied with power.

Choosing which lock type to use depends on the area you're securing. Entry doors call for fail-safe locks since they need to comply with building codes and fire regulations that require people to be able to exit at any time, even in the event of a power outage. IT rooms should be wired fail-secure because they need to remain locked at all times, even in the case of emergencies. Fail-secure doors also need to be equipped with electrified push bars to allow people to exit quickly in case of an emergency.

Access control panel (or controller)

The access control panel serves as the central hub for managing access to secured areas. Most people are not aware of its existence because it's usually installed in the IT room or the electrical, telephone, or communications closet. When someone presents a valid credential at the door reader, the panel receives the request to unlock a specific relay, connected to the specific door wire.



»Kisi's Controller Pro 2 + Wiegand board«

The Wiegand board is the perfect add-on when you want to upgrade your current access control system. It enables you to lift your on-premise access control to the cloud to enjoy additional functionalities like remote and global access management and automated workflows. The Wiegand board allows you to save time and scale across your organization. The installation is simple, with zero downtime during migration and no need for wiring replacements or hiring expensive contractors. You can choose which parts of your legacy access control system you'll keep, like readers and credentials.

Access control server

Modern access control systems do not need a local server since everything is hosted on the cloud. This setting provides an additional layer of security, lower costs, and a simpler, more streamlined user experience.

On legacy systems, where a locally-hosted access control server is used, there is typically a dedicated machine that runs the access software. The administrator can't manage it remotely but needs to be on-site. Since having to contend with several local servers can become complicated for managing hybrid and multi-facility workplaces, most modern companies upgrade to cloud-based solutions.

Infrastructure components

Low-voltage cables

Cables are a critical part of access control and can be one of the biggest expenses when purchasing or upgrading an access control system, so they should never be overlooked. When building out space, it's important that all the cables are specified so that the general contractor knows what to do. If the cables are not planned, you will need to add them later, meaning someone will have to lay cables or drill into the walls.

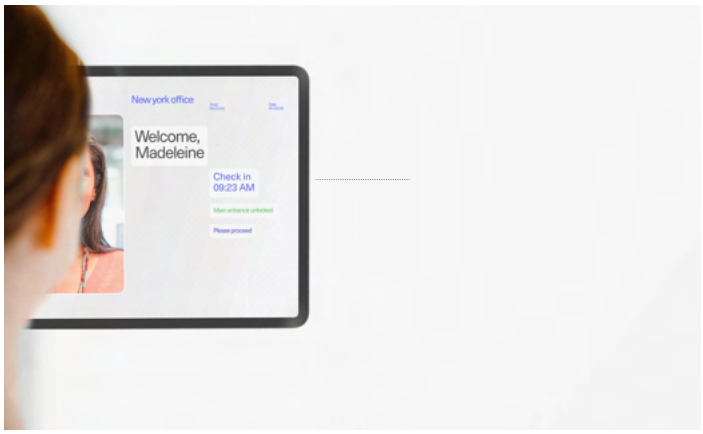
Two-wire switch and adapter

You can modernize your access control system and upgrade to the Kisi platform at a minimal cost while keeping your existing wiring. With the Two-wire Switch and Adapter, you get to enjoy all the benefits of an industry-leading access control solution with minimal installation costs. No need to pull new CAT6 cables to connect your future-proof Kisi readers. These accessories enable you to scale easily and securely by adding new doors and users with just a few clicks.

Kisi allows for a cost-efficient upgrade to cloud-based security with zero downtime.

Download our ROI document to learn more.

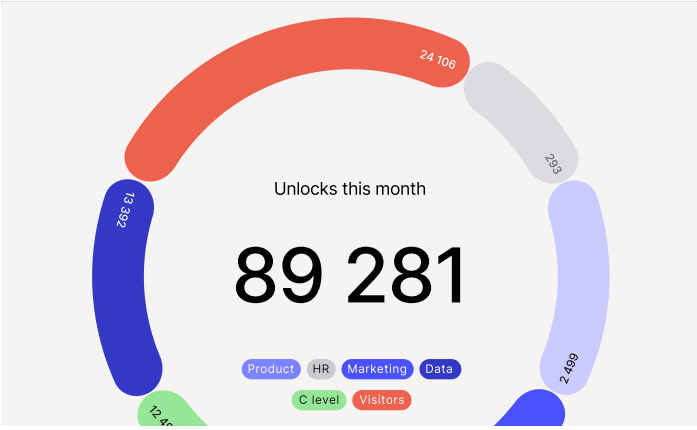
Access control benefits



Enhanced physical security

The most obvious advantage of access control, since it prevents unauthorized people from entering your building and ensures other interactions are perfectly regulated. For instance, modern access systems enable you to manage visitors and set access groups and schedules for different user groups like full-time employees, contractors, and vendors.

You also have control over all secured areas of your facility, so you can ensure only certain people can access specific spaces, like archives and server rooms.



Monetization with data insights

No matter the type of facility you manage, you can drive revenue with Kisi. For instance, membership businesses, like coworking spaces and gyms, can transform their business into a 24/7/365 unmanned facility. Setting different user groups with appropriate schedules or integrating with your software and synching your membership levels with Kisi ensures you only serve paying members who can only access the amenities they subscribed for without needing staff to manage the entrances.

You can also use Kisi's advanced reporting to optimize space utilization. This is especially useful for companies that use hybrid work models. With Kisi, you will have reliable data on exactly how many employees are coming to work on different days, which spaces they use during which times, and much more. Many companies use the insights of the Kisi data to make fact-based decisions on repurposing their spaces.

Explore the ROI-calculator for coworking.

Learn more

Access control benefits

Compliance

Compliance is a big driver for companies to upgrade their access control system. For instance, in case of a breach, many security managers can get into trouble if they don't comply with a series of certifications. Having a certified access control system like Kisi increases your credibility, makes you safer and better protected against malware and hackers, and ultimately leads to increased revenue. Access control is vital for compliance in many instances, such as:

- Hospitals, doctors' offices, and health insurance companies need to comply with HIPAA health data regulations.
- Banks, insurance companies, and any business that accepts and processes credit cards are subject to PCI credit card data regulations.
- SaaS providers, data centers, or any company hoping to maintain SOC2 cybersecurity standards.

Streamlined operations

Modern access control systems like Kisi integrate with your directories, allowing for automated user provisioning and de-provisioning. This means that on- and off-boarding processes are automatically taken care of from an access management standpoint. This reduces maintenance and manual tasks for your admins and also decreases the chances of human error, such as former employees or contractors still having access to your secured spaces. By automating access control you can reduce operational costs and save around $100 per person in the first year.

Visitor management

Access control also streamlines visitor management procedures by ensuring no visitor has access to your facility without being previously authorized by an admin. Kisi, for instance, enables you to send access links or QR codes to allow one-time users, visitors, and temporary staff to unlock doors in your place without the need to issue credentials or download an app.

To enhance security, you can also set a validity time for the temporary credentials and only allow access on selected doors. Managing visitors via your access control system improves the experience for both admins and visitors, assuring your business always leaves a good impression from the door.

IP and data protection

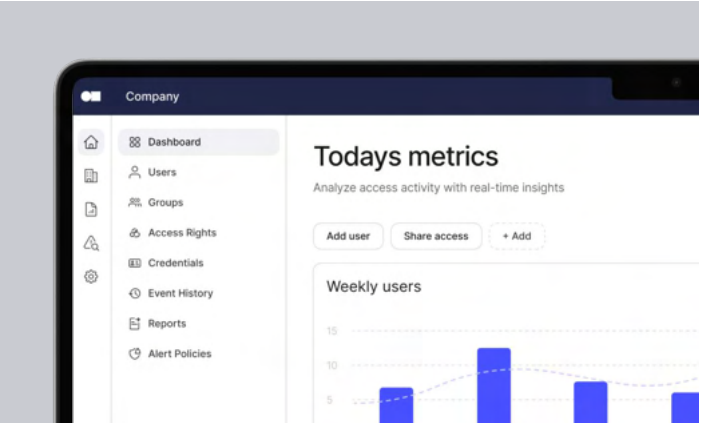
Businesses dealing with privileged data and intellectual property, such as software developers, law firms, entrepreneurs, and pharmaceutical companies, need to not only control who comes into their facilities but also which areas these individuals are allowed to access and when. Modern access systems allow granular permissions based on group memberships, and provide insights, analytics, and reports often required for both business and compliance reasons.

User experience

Access control systems nowadays need to enable businesses to create a highly secure yet welcoming environment. Adding additional barriers to how users access a facility, might discourage the modern, often hybrid workforce from spending more time in person. Leveraging technology that offers a smooth access experience and higher control on the admin side can support the return to the office and promote collaboration and productivity opportunities.

Implementing mobile access means empowering users to unlock any doors they have access to using their phones. They wouldn't need to fumble through pockets or bags to find the fob or write awkward Slack messages that they've forgotten the card at home. Advanced mobile access tech, like Kisi's MotionSense, takes convenience to another level by enabling users to unlock doors with a single wave of their hands in front of the reader.

Moving access control to the cloud



The access control market had been relatively stable for many years, with companies offering standardized products that relied on the same technology. Then, the cloud disrupted the industry, creating a duality of offerings: Legacy on-premises solutions (which do not work with a cloud infrastructure) and cloud-based access control systems.

Talk to our security experts to learn more about the difference between legacy and cloud-based systems, and the smoothest way to migrate to the cloud.

Learn more

Legacy vs. cloud-based access control

Legacy access control systems require a server to function, which implies having a dedicated server room with at least one employee responsible for maintenance. Besides the bigger upfront and operational costs, legacy systems also often necessitate higher facility costs and, due to their rigidity, are connected to slower innovation.

Cloud-based access control systems, on the other hand, don't require space when installed and can be used immediately after installation.

The main pros are remote, centralized management, mobile management and unlocks, and constant Over-the-air (OTA) updates by the service provider. As a cloud-based system, Kisi launches multiple OTA updates every month, ensuring your system improves continuously and will never be obsolete. Take a look at the main differences between legacy and cloud-based access control systems in the table below.

Legacy access control systems

- Requires own server/server room
- Challenging to scale across locations
- Higher maintenance costs and need for hiring a professional for doing this maintenance
- Fewer integrations, most of which require custom development
- Lower recurring costs but higher upfront costs
- Admins need to be on site or connected to a local network to manage
- May require additional measures to ensure compliance with industry standards
- Outdated UI, complex to manage, necessitating admin training

Kisi cloud-based access control system

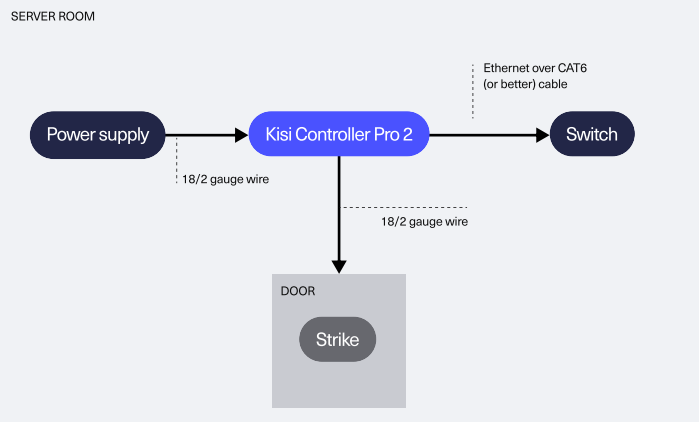
- Lower upfront costs and tailored migration options
- Automated OTA updates (future-proof)
- No need for hiring staff or dedicated customer service
- Integrates with multiple software and hardware and offers open API
- Mobile app and credentials
- Remote, centralized management
- Compliance with industry standards
- User-friendly interfaces with intuitive controls

Deployment options

Moving to the cloud might seem challenging or costly even if you already have an access control system in place. Kisi provides various deployment options tailored to your needs, budget, and preferences, considering the specific features you need and your existing legacy hardware and wiring.

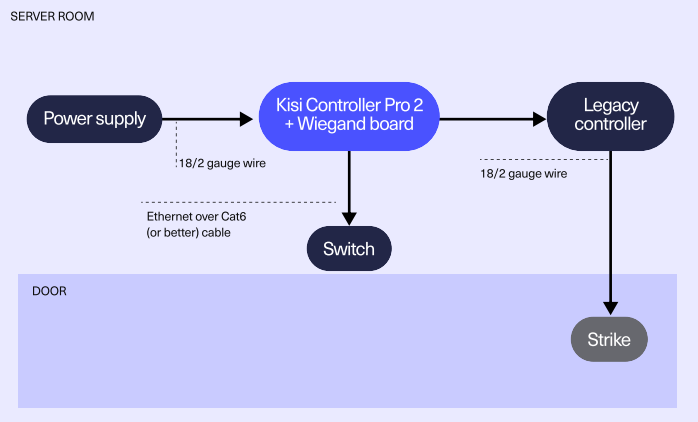
Mobile overlay

A. Mobile overlay



The perfect solution if you want to do minimal hardware and installation and still swiftly manage access through an intuitive cloud-based system. No need to mount readers or issue physical credentials like cards and fobs. All you need is a Kisi Controller. Admins enjoy Kisi's comprehensive features unrelated to the reader, while users can unlock doors with their phones using the top-rated Kisi app.

A1. Landlord scenario with mobile unlocks



If your office is part of a multi-tenant building, the main building entrance probably uses a legacy access control system you have no control over. In this case, the users have to carry two sets of credentials or use two different access methods to enter the office. With Kisi, you can ensure continuous access from the entrance to the office door, enabling users to use only the Kisi app on their phones.

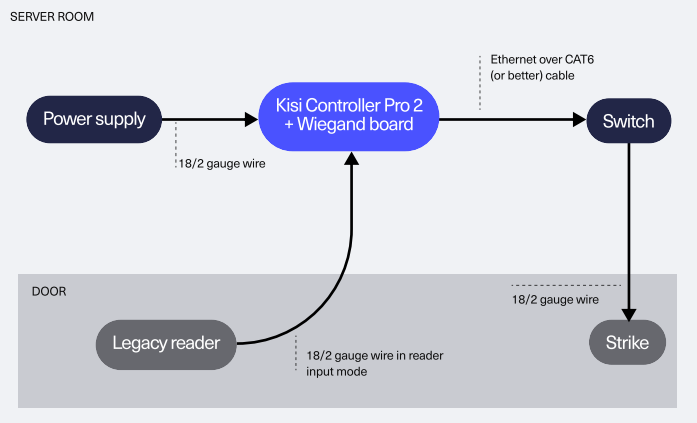
By simply wiring the existing legacy controller to the Kisi controller, you can allow for a seamless and secure transition between the two doors while the landlord can still maintain the legacy system's functionality.

Mobile and physical credentials overlay

B. Mobile and physical credentials overlay

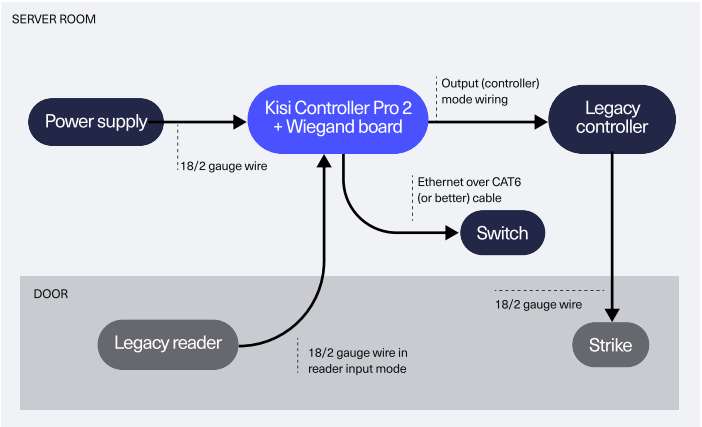
If your space or office building already has an access reader or controller in place, you might want to keep their functionality while moving to the cloud and enabling mobile access. Explore the options below if you want to continue using the fobs or badges or facilitate smooth access through the whole building without convincing the landlord to change the system.

B1. Keep legacy readers



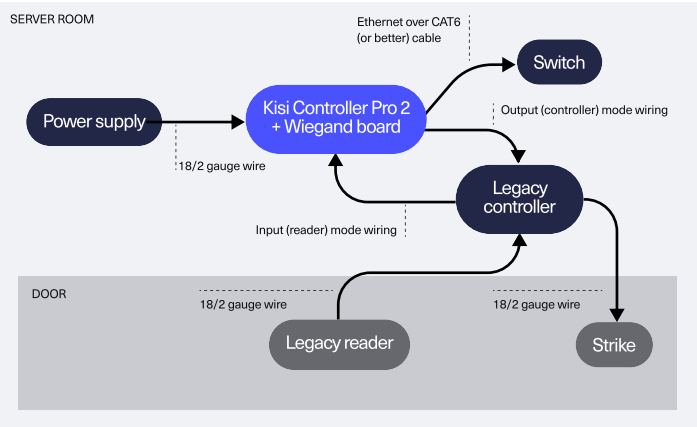
Keep your legacy readers and credentials for a cost-effective and efficient migration to a cloud-based access control system. Enhance security and convenience and enable mobile in-app unlocks without disrupting existing operations.

B2. Keep legacy readers and controllers



Choose this scenario if there are functionalities of the legacy controller that you must preserve, like alarms and fire alarms and you want to reuse your existing readers and credentials while enabling mobile in-app unlocks. Integrate Kisi with your legacy reader and controller, while maintaining your existing strike wiring to the legacy controller. Configure Kisi to decide how to handle unknown credentials - reject or pass them through to the legacy system.

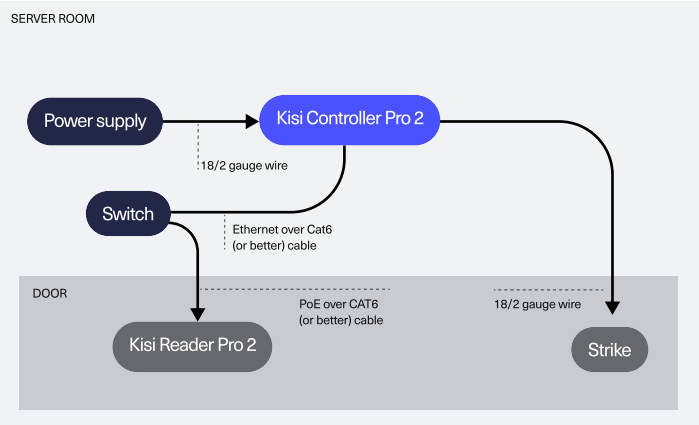
B3. Landlord scenario with mobile and physical credential unlocks

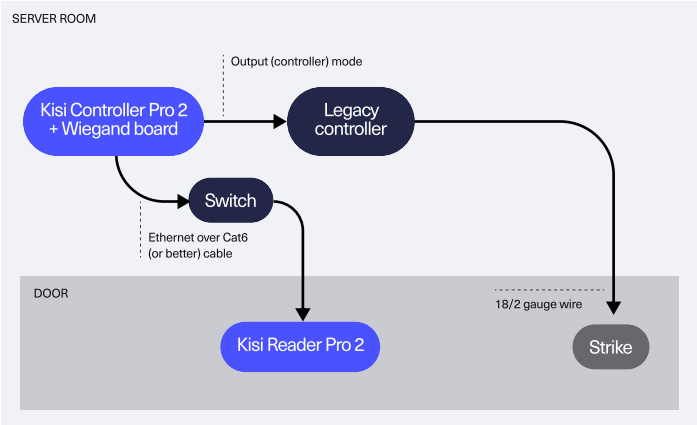


Ensure continuous access from the entrance door as a tenant in a multi-office building, even if the main entrance door uses a legacy access control system. Wire the existing legacy controller to the Kisi controller to utilize Kisi's card and mobile tap in-app unlocks to unlock the main entrance. The landlord's system's functionality will be intact, and building management can issue and control the credentials centrally, allowing for streamlined administration and updates and minimal landlord pushback. This also contributes to easier onboarding for new tenants and efficient handling of credential changes.

Full or hybrid Kisi deployment

C1. Using CAT6 cable

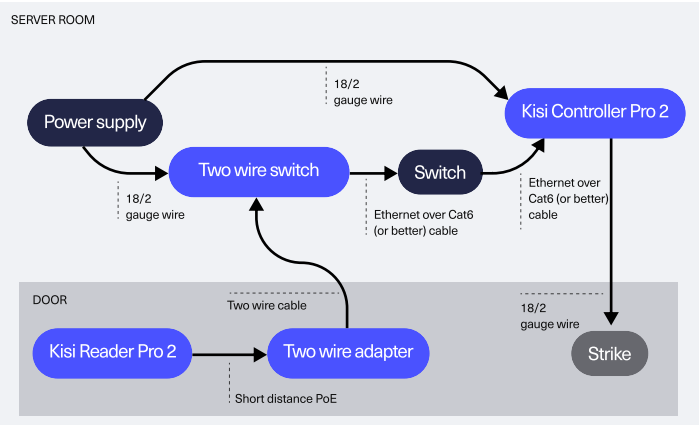


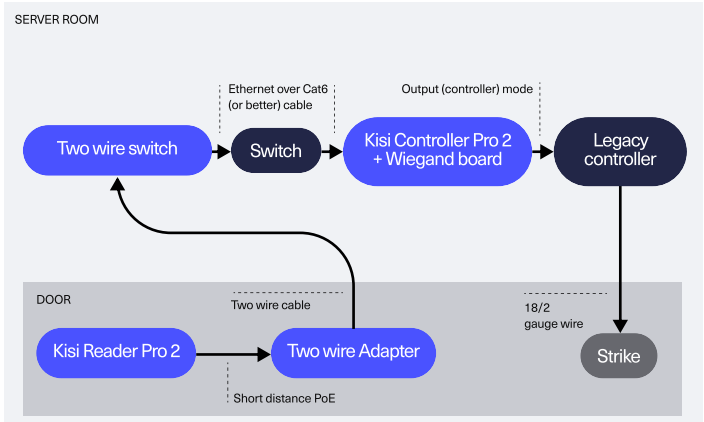


The state-of-the-art flavor of Kisi, our full deployment with CAT6 cable, is ideal if you're starting from scratch or looking to completely replace your existing access control system. Experience the power of Kisi with all its comprehensive features for a seamless and robust access control solution from day one. Choose between the Reader Pro 2 and the Terminal Pro for extensive access methods, including contactless unlocks with MotionSense, employee badges in Apple Wallet, and QR codes.

You can get the same functionalities even if you decide to keep your existing controllers intact and upgrade your access control system by replacing legacy with Kisi readers. With new CAT 6 cabling for each reader, you can enjoy the full range of features while using Kisi as a shared system of record for credentials.

C2. Keep existing wiring





Reuse and keep your existing wiring infrastructure intact with our two-wire adapter while fully enjoying the benefits of Kisi and bringing high-speed Ethernet to the edge for future-ready setups. This cost-effective migration provides a seamless transition to Kis i's with no additional re-cabling cost, empowering you to choose between the Kisi Reader Pro and Terminal Pro based on the functionalities you need.

The two-wire adapter enables you to maximize the value of your existing controller as well while preserving your current infrastructure investment. You can seamlessly integrate Kisi into the legacy system and operate both systems in parallel, leveraging Kisi as a shared system of record for credentials.

Access control software and hardware integrations

Cloud-based access control systems can be integrated with various software and hardware to streamline operations and enhance security. Explore the main access control integrations below and take a look at Kisi's ever-expanded integrations library for a more comprehensive view.

Video surveillance integration

Pairing access to your cameras and video management bolsters your security system. By reviewing access events with screenshots from the security cameras from your access control dashboard, you have a clear understanding of who is accessing your door and get visuals in case of a suspected security breach, like a door being propped or held open. Having this video surveillance solution in place will let you expand your security ecosystem and ultimately make your facility safer and compliant.

Directories and identity providers

Integrating access control with directories and identity providers saves maintenance time for admins by automating part of the onboarding and offboarding process while also reducing the risk of human error. This way, the new members you add to or remove from your directory (managed through your SSO provider or CRM) are automatically added or removed from Kisi. For instance, new hires can gain access to the right doors on their first day, improving the onboarding process, and you enhance security by automatically revoking access credentials when members move on. This keeps your office secure, welcoming, and up-to-date, with no additional maintenance required from your admins.

CRM and membership management systems

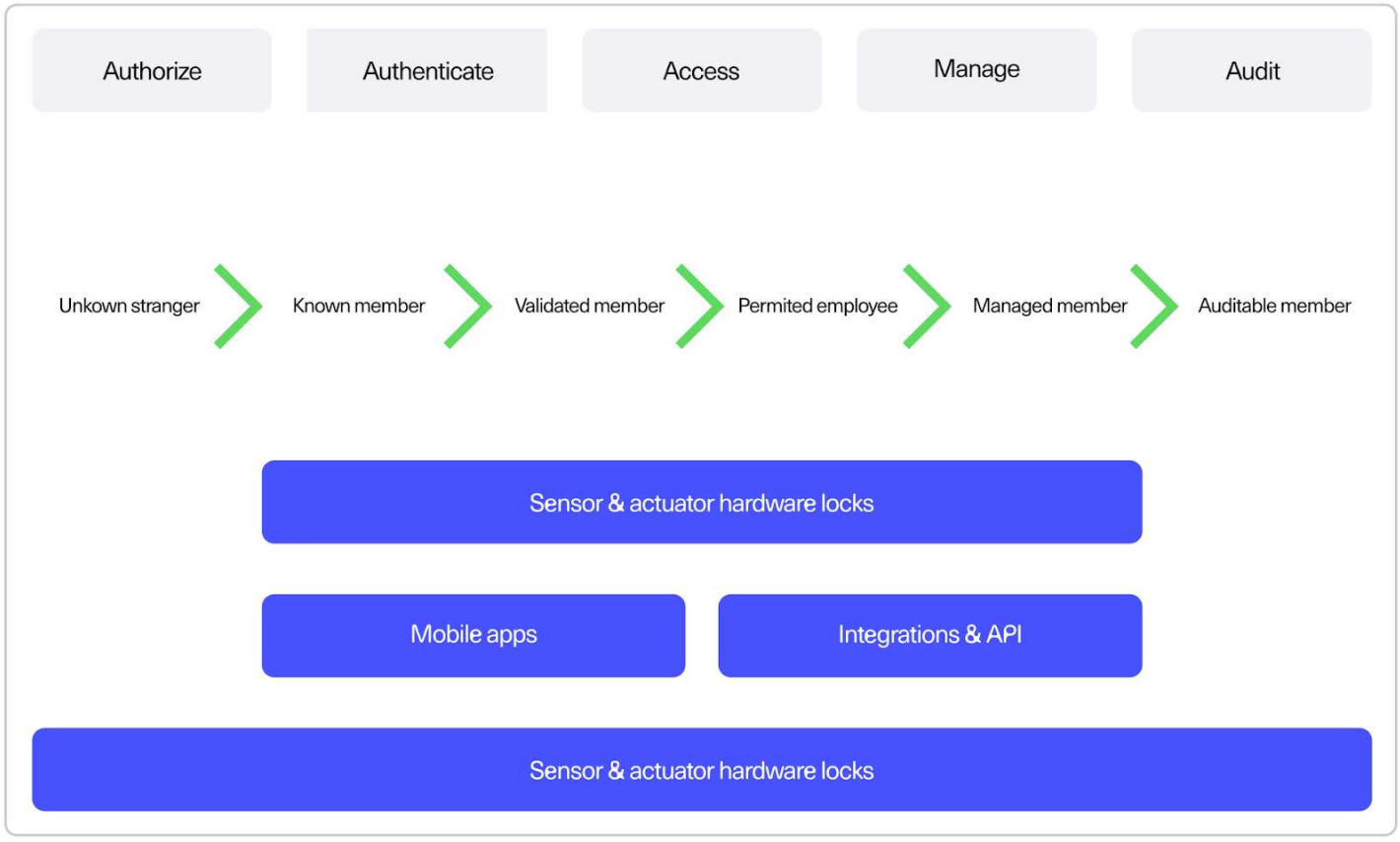
Particularly important for membership-based businesses, like coworking spaces, fitness facilities, or recreational clubs, integrating access control with an industry-specific membership management system automates access control, as everything is seamlessly managed through the CRM. Such integrations not only reduce operational overhead, like automatically revoking access to non-paying users or differentiating access restrictions by membership tier but can also open up additional revenue streams, like extending opening hours or unmanning spaces without hiring extra staff.

Hardware compatibility

Connecting your access control system to a fire alarm panel, an elevator board, or a temperature scanning device may be a requirement for a variety of businesses. Aside from the core features of a system, it is important to also consider compatibility scenarios with the existing tech stack and setups in your building.

Access control methodology

In our world of on-demand availability, access is extremely important and often taken for granted. While it's easy to say, "I'd like to restrict and control access, that's why I'm looking at access control," the question should actually be, "How should we set up access control to enhance user experience yet provide the secure controls our business needs?" Modern, cloud-based systems like Kisi don't only keep places safe, but invite the right people in.



The five phases of access control methodology

1 Authorization: Stranger to member

Authorization is the phase that turns strangers into members. The first step is defining a company policy which determines what people can and cannot do, including who has access to which door(s), during which times, and whether members of the organization can share access.

The next step is role-based access control (RBAC). By assigning roles to users, they get a certain set of assigned privileges. This comes in handy for administrators since they don't have to individually update every user in case of a change. Most organizations use employee directories in tandem with RBAC since these lists include all authorized employees and their access levels.

2 Authentication: From member to validated

Authentication goes one level deeper than authorization. In this phase, members present to a door reader whatever badge, token, or credential they were given upon being authorized. The reader will check its validation to determine whether or not it should unlock the electric lock on the door in question.

3 Access: From validated member to access

Now that the credentials have been authenticated, the access tools available at this stage ensure everyone swiftly gets in the right door at the right time.

Unlock: Upon validation, the presenter can unlock the desired object, like a door, elevator, or cabinet. This can happen by pushing a button or presenting a mobile device, access card, fob, or badge that requests access.

Trigger: Once the access control system has received the request to enter, the access is triggered, typically in the form of a door unlock.

Infrastructure: If the door unlocks, multiple events are tracked at once: The user was correctly authenticated, the user triggered an unlock, the door opened, and the door closed.

4 Manage: From access to monitor

This phase helps the administrator meet several challenges, including adding new access points, onboarding and offboarding users, maintaining security, and troubleshooting problems. Let's examine some advantages.

Scale

Cloud-based access control systems can help startups and small businesses move to new or expand to additional offices by providing flexible and modular extensions of the existing setup.

Monitor

Online access control systems send real-time alerts to administrators or security should any irregularity or attempted breach take place at any access point, allowing them to investigate immediately and record the event.

Troubleshoot

Modern access control systems allow administrators to remotely configure permissions or seek support from the vendor should access points or users have issues—a huge advantage over locally-hosted systems.

The five phases of access control methodology

5 Audit

Auditing physical access control is useful for all types of businesses. In addition, it helps certain sectors meet special requirements.

Scale

Businesses can perform regularly scheduled system reviews to make sure everything on the access control system is set up properly. It can also tell them if someone no longer employed by the company has been inadvertently left in the system.

Suspicious events

Since many access points are routinely tracked during any access event, auditing can prove useful to security officers when investigating unusual behavior. The data can be used to flag or highlight unusual access behavior or analyze it against historical data.

Compliance reports

Companies that process sensitive data like patient healthcare information, banking financial reports, or credit card payments must deal with audit requirements in the access control space when filing compliance reports in accordance with HIPAA, SOC2, or PCI. Some special categories like cybersecurity or ISO certifications also require managed and auditable access control. The audit phase can pull up the proper data for these periodic reports.

How to set up your new access control hardware

If you already have an access control system in place, the setup process can be different based on your migration path. Contact our security experts for a detailed, customized walk-through.

But what happens if you're installing an access control system from scratch? How does the system get installed in your space?

Typically installers take a few days from confirmation of the order until the actual installation because they need to order the required parts. Once you have an actual installation date, the installer will follow the process below.

1 Run the cables

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

2 Install the readers at the door

Most readers just need to be screwed on the wall and connected to power. Modern readers, like the Kisi Pro 2, need an internet connection, too.

3 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 to see that all doors unlock correctly.

4 Install the access control panel in your IT room

Most access control panels can handle multiple doors. The integrator might install a backup power supply, or other additional security hardware, depending on your building's specifications.

5 Install the locks

Unless already in place, an 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 this step first so the office workers are not annoyed in the middle of the day.

Introducing the access control system

Set up users, groups, and door access schedules

When should certain doors unlock? Which types of access groups or individuals should be able to gain access? The door access schedule can evolve into an important discussion: Are IT managers 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, facility, and management teams, since these are the rules that your security strategy will be based on and it will determine what you actually want to control.

Test the system with a few pilot candidates or coworkers

Try running through the process that you envision for every employee or visitor with a smaller sample at first. Provision access for them, activate their access, hand over the access card, or share mobile access with them, then ensure it runs smoothly. If you roll out your process too quickly, you might have some smaller hiccups. The more people you involve, the faster it can escalate.

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

Run through all possible scenarios when you want the user not to be able to unlock the door. For instance, many offices get broken into during vacation days. Some offices automatically unlock their doors during workdays. If the workday is a public holiday, burglars know they might just be able to walk in. Some systems, like Kisi, even offer automated holiday schedules.

Announce the roll-out

Send an email to everyone to announce the change in access control. Some people might not like change. Yet even if they have an emotional bond to their physical key, implementing a mobile access solution that offers more convenience can convince anyone. You can remind users that using digital credentials not only allows them to enter places without fumbling through pockets, but they can also rest assured knowing they won't easily lose or displace their credentials.

Onboard your team

Once the system is tested, announced, and approved, the exciting part begins: The actual rollout. You can start provisioning access for your team. The most important part to consider is that some users might 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 that there's time to troubleshoot.

What to look for when choosing an access control system

There are several factors to take into consideration when comparing different providers. Below is an overview of some of the main questions you may want to look at.

Compatibility

Compatibility is very important when choosing an access control system. Making sure that the system you want to purchase is compatible with your facility can save you a lot of time and money during the installation process. A highly compatible system, like Kisi, also makes it easier to maintain the facility and ensure a high level of security. Some compatibility-related questions may be:

- Is it compatible with third-party hardware and free from lock-in?
- Does it integrate with video surveillance and other security systems?
- How easy is it to use and configure?
- Does it offer an open API?

Features and maintenance

Features are obviously essential when choosing any type of security system for your space. What can be challenging is understanding which features need to be prioritized in order to find a solution that not only covers your basic needs, but also saves you time and resources in the long run.

We recommend choosing a cloud-based system with multiple unlocking options (not limited to only keycards or fobs). This enhances user experience and reduces operational overhead, as you don't have to issue a new keycard every time there is a new visitor or employee. It also reduces the number of security issues caused by employees forgetting or misusing keycards and fobs.

Lastly, we would recommend choosing a company with solid customer service so you can quickly clear any doubts that might emerge during installation or everyday use of the system. Some other feature-related questions you should consider

- Is the hardware IP-based?
- Is offline mode supported?
- Is two-factor authentication (2FA) supported?
- Is lockdown supported? If so, is it at door or place level, or both?
- What communication channels does it run on (e.g., Bluetooth, NFC, RFID, PoE, and others)?
- Does it support multiple types of authentication input such as mobile apps, remote unlocks, cards, key fobs, and more?
- Are all access methods offering end-to-end data encryption?
- Is customer support included?
- What access restrictions are available (e.g., time-based access, role-based access, level-based access, count-based access, and others)?

Overview of key Kisi features

Kisi is an ever-evolving platform offering the most advanced features on the market. Thousands of businesses use Kisi every day to manage access to their facilities, provide a secure environment to their employees and visitors, and streamline workflows and operations.

CREDENTIAL	USE CASE
MotionSense	Unlock doors by simply waving your hand in front of the Kisi Reader Pro 2 or Terminal Pro. No need to have your phone on hand.
Employee badges in Apple Wallet	Add your Kisi credential to Apple Wallet and use your iPhone or your Apple Watch to securely enter spaces.
Tap to unlock	Unlock doors in less than a second by tapping the phone against the Kisi reader.
In-app unlock	Unlock Kisi-controlled doors in seconds with a tap in Kisi's top-rated mobile app.
QR codes	Scan your QR code with the Kisi Terminal Pro for effortless, user-friendly, temporary access.
Cards and fobs	Use Kisi cards or your legacy NFC or RFID badges or fobs for a swift unlock experience.
Scheduled unlock	Set your doors to be open during specific windows of time.
Visitor links	Tap the link you get via email, text message, or chat app to unlock specific doors during a set time.
2FA mobile access	Add an additional layer of security by enabling 2FA on mobile unlocks.
Elevator access	Extend Kisi's cloud-based security to elevators.
Badge printing	Integrate badge printing capabilities for easy and secure visitor identification.
SAML based SSO	Integrate door access with your SSO provider.
SCIM for access provisioning	Seamlessly keep your user information up to date across all platforms.

Security and access management

TYPE	USE CASE
Access groups management	Create different access groups to automate access sharing and enhance security.
Roles management	Set different levels of management for your admins per place, group, or door.
Access restriction	Set granular access permissions and time-based, device, nearfield or location restrictions.
Automated provisioning	Automate provisioning with Kisi's directory integrations.
Global management	Unlimited doors, places, and users, all from a single dashboard.
In-and-Out tracking	Installing Kisi readers on both sides of your door to track exactly when someone enters and exits your facility, even without using the Kisi Controller.
Intrusion alerts	Set alerts for when a door is held open or forced open.
Lockdown	Secure any door remotely by using Kisi's lockdown feature.
Remote access sharing	Share access with anyone, anywhere thanks to our remote management features.
Remote management	Validate entries and manage your space remotely 24/7.
Offline mode	Unlock doors even when your network is offline.
Visual access audits	Integrate video surveillance to review and validate door entries with automatic video snapshots.
Open API	Developers can use Kisi's open API documentation.
Access teams management	Create different access teams to automate access sharing and enhance security across all your places.

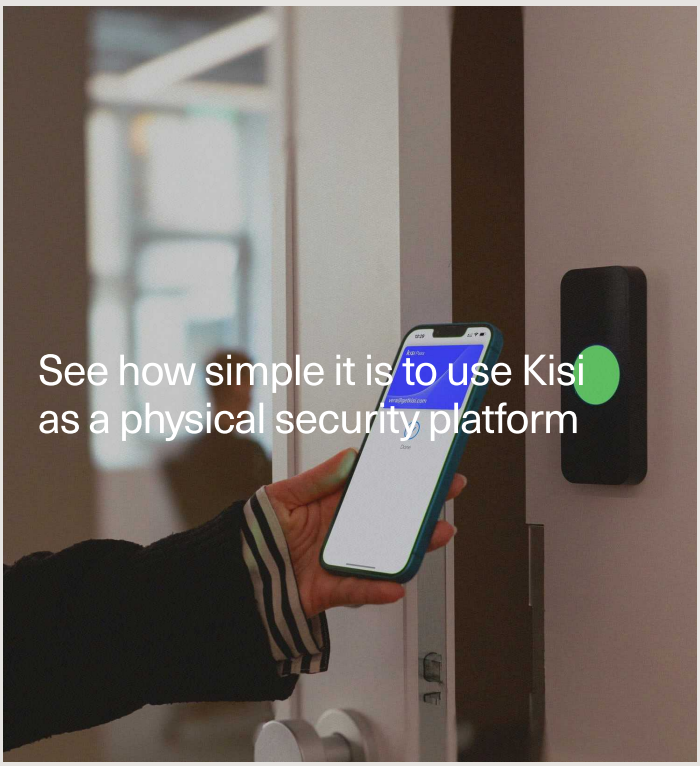
Analytics and reporting

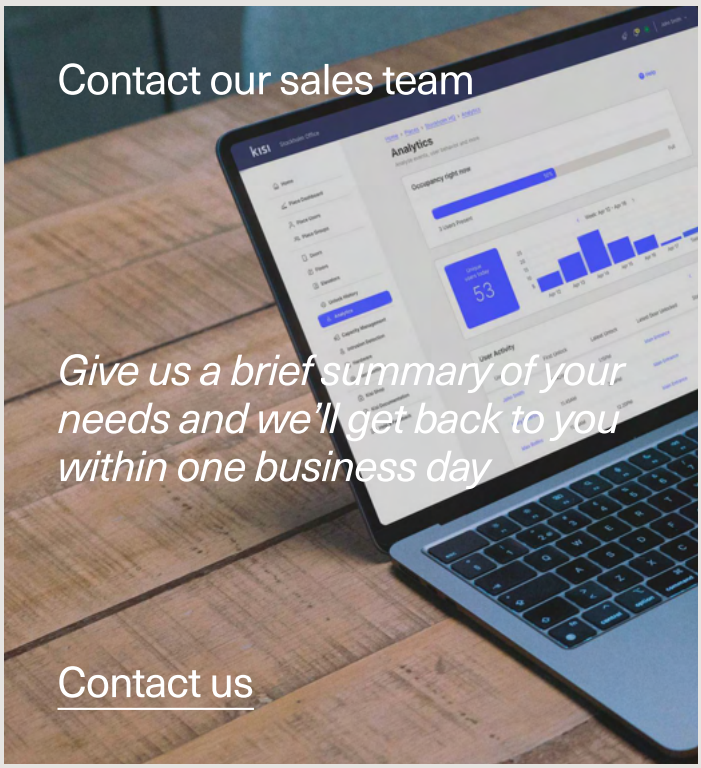
TYPE	USE CASE
Detailed event history	Review a thorough and chronological record of every access event, like door unlocks, doors held open, and door lockdowns.
User behavior insights	Detailed analytics for any user directly from their profile. Track arrival patterns, total days on site, and daily presence.
Place analytics	A comprehensive view of your facility's activity, including current occupancy rates, user behavior, and detailed activity heatmaps.
Event exports	Locate and analyze specific events in your Kisi environment with advanced filters for objects and variables.
User exports	Locate and analyze specific users in your Kisi environment with a detailed list of user properties.
User presence reports	Track unique unlocks and active days within a set period, with options for organization-wide or location-specific data.
Weekly place analytics reports	Track daily place usage, heatmaps of unique user unlocks, weekly unique users, unlocks by credential type, top 5 most used doors, recent failed unlock attempts, and hardware metrics.
Door unlock permissions	Get a list of users with access to a specific door, including their name, email, role, role scope, and permission validity dates.
Custom reports	Request any custom report tailored to your specific needs.

*See all features based on pricing plan

Kisi security platform

As the highest-rated access control solution, Kisi is securing thousands of businesses across the world, from high-tech companies like Canva to U.S. Air Force facilities. Our advanced features are setting new industry standards and are built to provide an incredible access experience to both admins and end-users.





45 Main Street,
11201 Brooklyn
USA

sales@getkisi.com
getkisi.com