

Product Overview

Reader Pro / Controller Pro

Unified Enterprise Access Control for Facilities



Introduction

Kisi offers simplicity and added security to organizations looking to modernize their approach to physical security. The Kisi Pro line, including the Reader Pro, are available in indoor (KRP50) and outdoor (KRP80) models. The Pro Controller (KCP50) eliminates the need for local servers, manual operations and localized standards—ultimately reducing complexity and lowering operating costs.

In place of the local server, each Kisi Pro Reader streams mobile or card credentials directly, via PoE through firewall for authentication, by the Kisi cloud. Once authenticated, the controller can trigger one of the four possible connected doors to unlock. Beyond that, the controller also acts as a control center for the doors; synchronizing door-open and closed events as well as exit tracking.

This fully encrypted and distributed design offers a number of unique benefits. It improves security by doing away with single points of failure and unmanaged local windows servers. It minimizes manual operations by streamlining the on-and off-boarding process and it greatly reduces the cost and complexity of expanding the system; new readers and controllers are simply installed without any additional hardware equipment required.

Paired with Kisi's intuitive web-based software, the Pro line comes alive with powerful new capabilities. It's easy to grant, edit and revoke access permissions for any user—by door, group or place. A real-time activity log, instant search and event exporting reduces hassle and speeds up response times.

Kisi makes it possible to remotely manage all devices, even down to the electronic components. Since the devices are cloud-managed, software updates and upgrades occur automatically. The result? Kisi devices are always up to date with the latest, secure firmware. without manual scheduling.



Table of Contents

04	MODERN, SECURE ARCHITECTURE
05	Kisi Reader Pro - KRP50 & KRP80
06	Kisi Controller Pro - KCP50
07	EASY MANAGEMENT
07	Powerful Access Control & Secure Remote Access
08	Flexible and Customizable Credentials
09	Future Proof - Built to Scale
10	POWERFUL INTEGRATIONS
10	Direct Integration With Your Ecosystem
11	Works With Any Existing Electronic Lock
12	STREAMLINED SECURITY
12	One Security Standard for Digital Tools and Physical Space
13	Full-Stack Control Without 3rd-Party SDK's or Local Servers
14	Real-Time Events and Predictive Alerts
15	FURTHER READING
15	Our Process
16	FAQ



Join the highest-rated door security platform:
sales@getkisi.com, (+1) 646 663 4880
www.getkisi.com

Modern, Secure Architecture

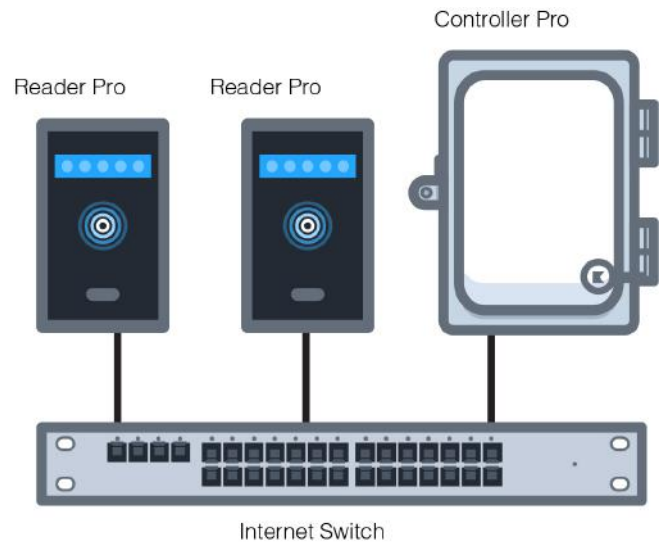
Kisi eliminates the need for local servers and manual maintenance, resulting in a system that is simpler, more secure and easier to operate and manage. Vulnerable protocols between reader and controller, which are common in traditional access systems, are omitted by design as all communications through the firewall first.

SUMMARY

- ✓ End-to-end encrypted communications architecture eliminates vulnerabilities by design
- ✓ Securely managed by the cloud, Kisi makes it easy to remotely manage and control all devices
- ✓ Management and credentials are available and changeable in real time, making operations fast and easy

Kisi devices are automatically self-secured straight out of the box. This safety layer prevents unauthenticated computers to communicate with the device even if they are on the same physical network.

Looking at an example wiring diagram of a Kisi setup including [Kisi Controller Pro](#) and [Kisi Reader Pro](#) shows a main difference to other systems: The wall reader is directly wired to the firewall, forcing incoming traffic to run through your security first before communicating with the panel.



Each device only communicates via documented encrypted connections, underpinning an efficient and secure architecture. Credentials that are read and communicated through the devices are encrypted with challenge response and public key infrastructure (PKI), which prevents unauthorized credentials; even in the unlikely event that credentials are somehow copied.

Kisi hardware is manufactured by U.S.-based manufacturing companies. As part of our rigorous production lifecycle, all firmware is cryptographically signed by Kisi to ensure that only authentic firmware can be uploaded to each device.

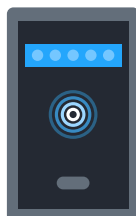
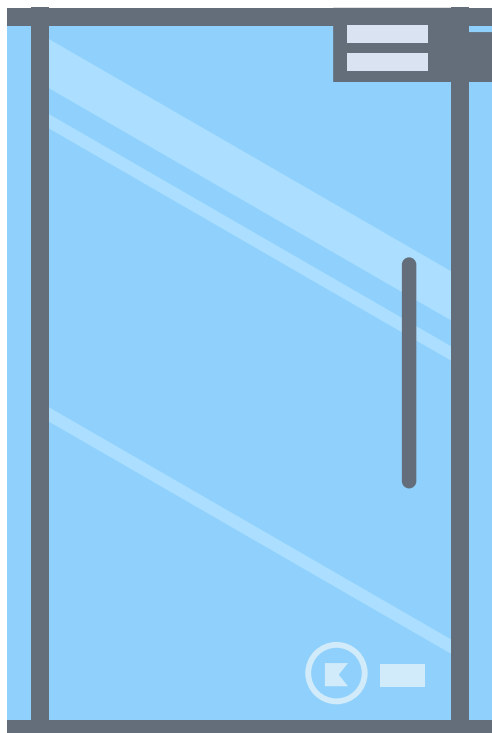
Lastly, Kisi works exclusively with datacenter operators that meet the highest industry standards for security and privacy including [ISO 27001](#), [SSAE16](#)/ISAE 3402 Type II, [SOC 2](#) & 3.

Kisi Reader Pro - KRP50 and KRP80

The reader is installed outside of the door to read user-facing access credentials such as [cards](#) or [smart-phone](#)-based credentials.

KEY FEATURES

- ✓ BLE / NFC wall reader programmable via [API](#)
- ✓ Power and internet via PoE or low voltage and WiFi
- ✓ Over-the-air updateable OS with potential for local cache



The user experience can be customized:

Using Kisi's mobile app

- Pull up the app to unlock the door, or:
- Hold the phone to the reader to unlock the door automatically without unlocking the phone using Kisi's "Tap-to-Unlock" technology

Using Kisi Passes to unlock the door

Kisi Passes are 128bit AES encrypted cards that are based on the MiFare DesFire EV 1 card platform

Read more about the Kisi Reader Pro:

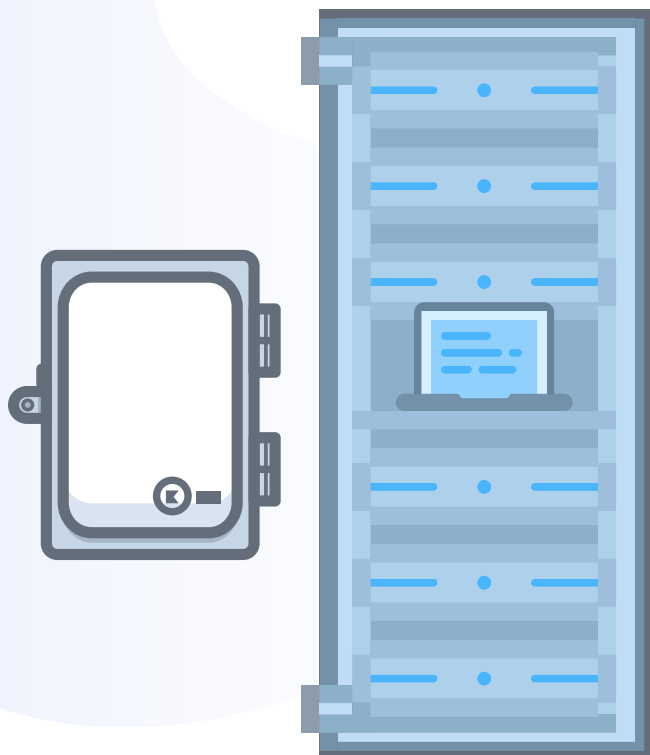
[Read More](#)

Kisi Controller Pro - KCP50

The controller is installed in the IT or communications room and connects up to 4 wired [electronic door locks](#) to their relays. For more than 4 [doors](#), the Kisi controller can be added as modules and scale up to an unlimited number of locks.

KEY FEATURES:

- ✓ 4 powered or unpowered door relays, 4 door contact sensor inputs, 4 push to exit inputs
- ✓ Power via Ethernet or WiFi
- ✓ Over-the-air updateable OS with potential for local cache



The administrator experience includes the following workflows:

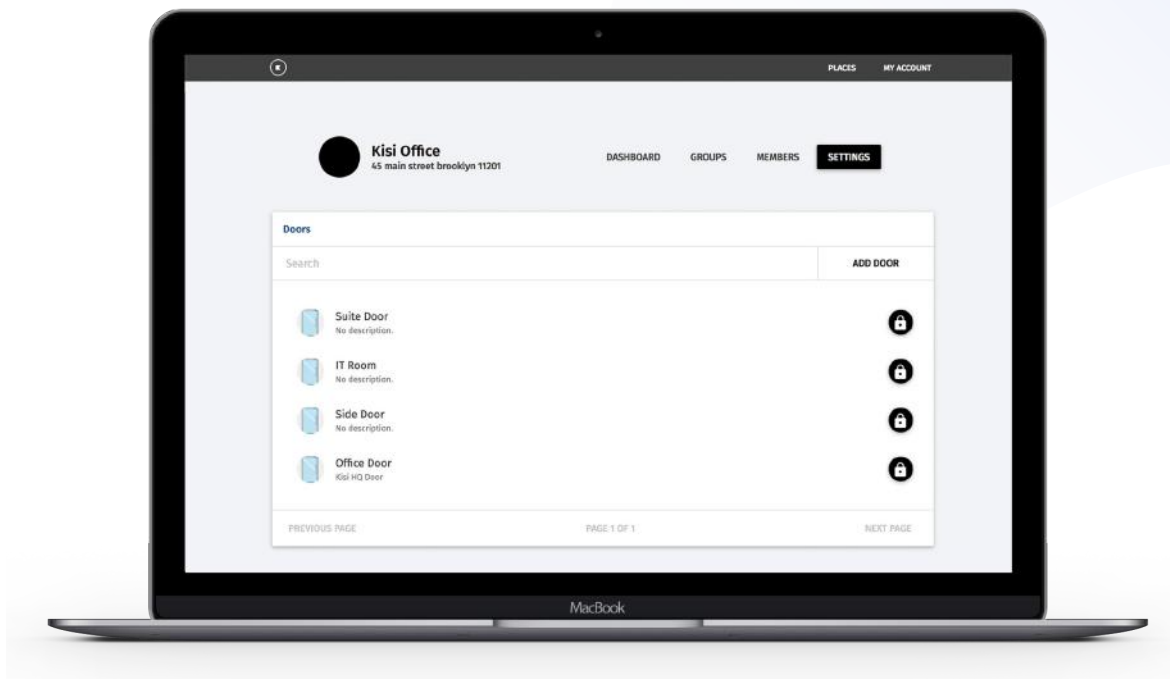
- Plug & Play connection
- Manage and see device status in the [Kisi Dashboard](#)
- Program all in- and outgoing connectors via Kisi's Dashboard

Read more about the Kisi Controller Pro:

[Read More](#)

Easy Management

Powerful Access Control & Secure Remote Access



Kisi's secure web-based application empowers administrators to easily and effectively manage access rights for their entire organization. Effortlessly grant and restrict user access to an individual door, pre-configured group or location, and apply user roles to establish an access rights regime that fits your organization's needs. Want to grant a new regional manager access to 5 locations? Kisi makes it straightforward and painless.

The software also makes it easy to securely share access rights and event logs of parties, such as vendors or guests, with approved third parties like law enforcement and legal professionals. Event logs can be exported and expiration-dated access can be easily granted. With Kisi, there is also the ability to remotely check the status of a door and unlock it remotely—a potentially life-saving feature during instances of active threats or prolonged security incidents.

KEY FEATURES:

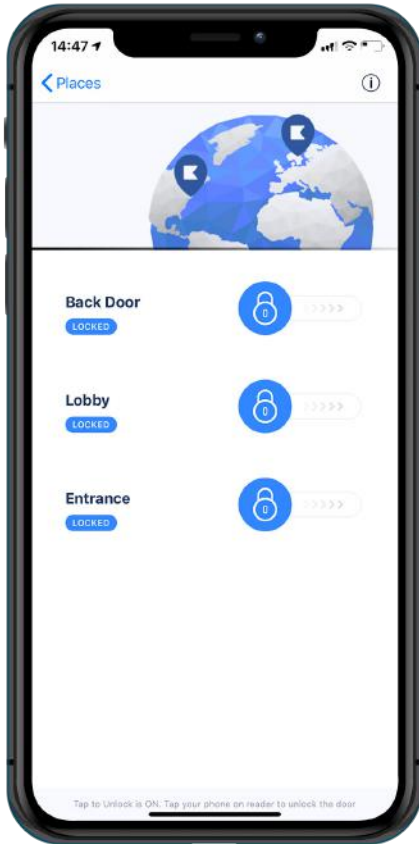
- ✓ Granular control for users, doors and locations
- ✓ Time-restricted access
- ✓ Detailed access logs

Read more about the Kisi Dashboard:

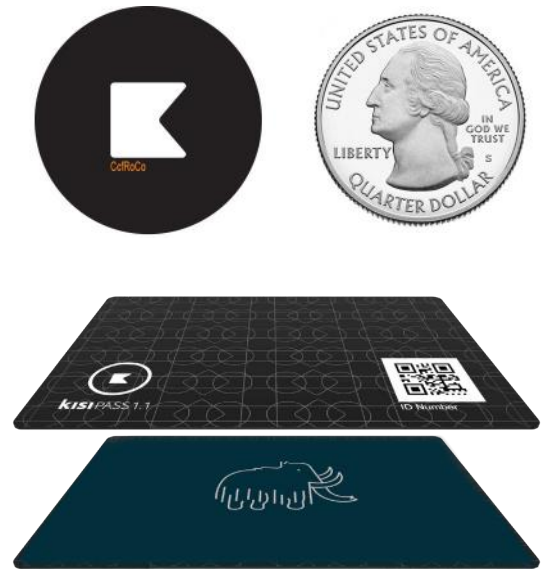
[Read More](#)

Flexible and Customizable Credentials

Getting in the office shouldn't be hard; however, it must be secure. That's why Kisi offers flexible mobile and physical credentials that offer different use-cases but don't compromise on security.



Smartphone credentials support iOS and Android with respective native apps. Since door access requires direct communication between phone and reader, we use [BLE](#) (Bluetooth) on iOS and [NFC](#) on Android. If you have your own app, it's also possible to include Kisi's functionality in it through the API. [Read more here.](#)



NFC cards and tags are built on the powerful MiFare DesFire EV1 standard, which is one of the best NFC smartcards. Building on that platform, we custom encrypt each hardware credential with 128bit AES encryption in our facilities so there is no compromise in security compared to using apps. Cards and tags can be de-activated anytime by the user in the mobile app, an additional security feature.

KEY FEATURES:

- ✓ Diverse credential methods in secure formats
- ✓ Branded credentials for employees
- ✓ End user can disable access

Read more about the Kisi credentials:

[Read More](#)

Future Proof - Built to Scale

Having a future-proof system is essential. No one wants the hassle of replacing their access system or locks and other hardware.

Unified Access Control

With most systems, you constantly need to transition as you grow:

- You start with a 'small-size' company system
- Then you need a 'mid-size' company solution
- Then you must upgrade to enterprise

It doesn't have to be that way. With Kisi you can start with a small POC (Proof of Concept), like limited deployment, without compromising functionality and security. When you're ready, you can then seamlessly scale up the solution across your facilities to unify your access control.

Over-the-Air Updates

Manually maintaining infrastructure is a task that no one really has the time for, and you can't easily do it remotely. That's why all of Kisi's devices receive over-the-air updates of signed firmware that includes the latest security updates and product improvements.

Credential Agnostic

The smartphone might be the most widely-accepted modern credential, but maybe in the future we'll use our watches, headphones or just our behavior to unlock the door via biometrics and blockchain encryption. Kisi's platform is ready to adopt future credentials as technology evolves, without changing your hardware at the door.



KEY FEATURES:

- ✓ Unify your access control at locations of any size
- ✓ Every device has an OS that's updated over the air
- ✓ Credential agnostic and ready for what's coming next



Powerful Integrations

Direct Integrations With What You Already Use

One of the largest benefits of going mobile with door security is the ability to manage credentials dynamically: Imagine if every time you added someone to your Active Directory they automatically received door access that corresponds to their access level. You can also add the Kisi app to your MDM for automated provisioning. Of course, this is even more critical when terminations happen as all credentials should be revoked in real time and in a predetermined, automated, manner.

That's why Kisi allows out-of-the-box integrations with the most popular Active Directory services such as [Microsoft Azure AD](#) or [Google Apps](#). We believe that allowing you to audit door access, like any other service you use in your setup, should be a standard feature in your security workflows.

KEY FEATURES:

- ✓ Out-of-the-box Active Directory integrations with Google or Microsoft Azure
- ✓ Audit door security like any other IT system

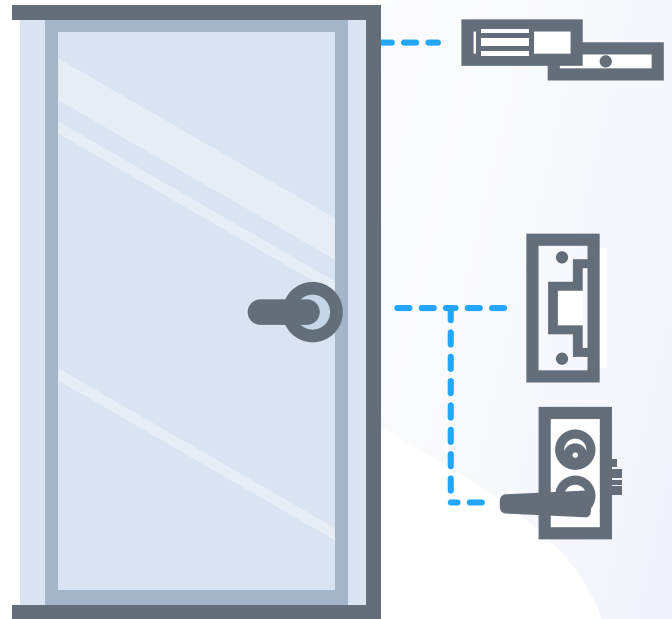


Works With Any Existing Electronic Lock

Every door and location is different. Sometimes you move into a space with pre-existing electronic door hardware; sometimes you build out your space. In either case, Kisi works with any wired electronic lock that is already pre-existing or about to be installed. This allows you to be flexible during the construction and planning phase and you can connect Kisi to the system later on without special requirements.

The components most relevant for common compatibility issues are:

- [Electronic locks](#): Typically doors use electric strikes, electronic mortise locksets or magnetic locks.
- [Wiring](#): The Kisi Reader Pro needs a CAT6 cable at the door while the lock typically runs on low voltage 18/2 gauge wire.



KEY FEATURES:

- ✓ Compatible with standard electronic locks
- ✓ Works with typical IT cabling



MORTISE LOCKS



ELECTRIC STRIKES



PANIK BARS

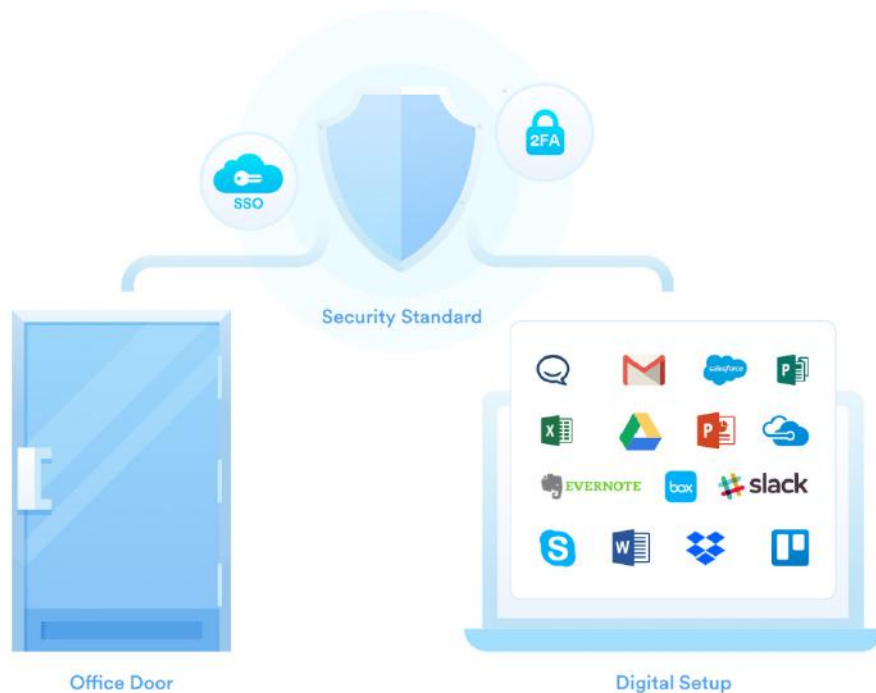


MAGNETIC LOCKS

Streamlined Security

One Compliant Security Standard for Physical Space

Kisi allows to expand SSO and 2FA to your Office



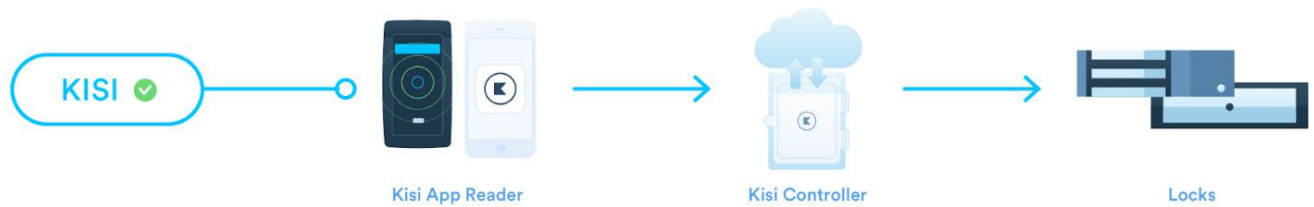
Most companies set up SSO (Single Sign On), such as Okta or 1Password, and [2FA](#) (Two Factor Authentication) for their apps to control security wherever the user might be. Why not include your doors in that setup? If you're running Okta, just connect Kisi to your Okta account and provision keys automatically from there. You could also potentially set up MFA (Multi-Factor Authentication) for specific doors like server rooms, executive doors or data centers to increase security.

This helps to make compliance audits for standards like SOC2, ISO, PCI, HIPAA (and many more) a lot easier. Read more about achieving different compliance standards [here](#).

KEY FEATURES:

- ✓ Extend a digital security setup to your doors
- ✓ 2FA on mobile makes app-based unlocks secure with BYOD
- ✓ Get doors under the SSO umbrella of the organization

Full-Stack Control Without 3rd-Party SDK's or Local Servers



Kisi's mobile technology does not rely on external SDK's such as HID. This allows us to perfect the experience and security faster than the market evolves. A simple example: Adding Two Factor security to our app doesn't require waiting for HID. There are no dependencies when one system updates and the other is not. We don't need a separate server to host the mobile credentials. These are all the things you wouldn't necessarily think of when comparing two access control system providers, but in practice it is a major difference.

KEY FEATURES

- ✓ No dependency on 3rd-party SDK
- ✓ Control end-to-end security
- ✓ No downloading or synchronizing of credentials

Real-Time Events and Predictive Alerts

Kisi's system generates data that can be used for getting security, workflow or user insights. For us, modern door security is really the first step. Using AI and machine learning will push facility security to the next level.

KEY FEATURES:

- ✓ Every device has an OS ready to be updated over-the-air
- ✓ BLE and NFC technology
- ✓ Credential agnostic

Here are a few examples of how you can use Kisi's data:

- Event log: Use the real-time event log to stream access data from unlocks with user name, lock name and timestamp to tie [door open and closed](#) events or [request to exit](#) triggers
- Heatmap: See how your space is used by looking at heatmaps of unlock activity in your space
- Alerts: Set alerts on groups, members, doors, etc.
- Predictive arrival times: Once the system has been used for enough time, Kisi understands the patterns of each individual and can predict arrival time windows. When an unexpected event might occur, you get notified. This is the first step to making door security as secure as credit cards.



Further Reading

Our Process

Our process starts with free training and setup by a certified Kisi installer:

1

First, we stop by for a visit.

A local, certified, Kisi installer checks out your space and decides what tools or hardware are needed. Kisi is compatible with any electrical-powered lock.

2

Get a final quote, tick all the boxes.

We'll send you a final quote, after we've evaluated your space, to build your custom access control system.

3

We'll ship your hardware.

We'll ship your hardware order via UPS, or DHL Express if you're abroad. Global delivery is possible within 24 hours—talk to our sales team to learn more.

4

Pre-installation begins.

We'll assign you a dedicated Kisi specialist who will answer all your questions throughout the installation and onboarding process. Your Kisi specialist is available anytime you have a question, even after the system has been set up.

5

Installation is complete.

Once your Kisi system is installed, your specialist will connect the controller to your door locks and help you set up your account(s), create doors and start issuing keys!

Read more about our process:

[Read More](#)



FAQ

Who provides the hardware and mobile credentials?

Kisi does not use 3rd-party SDK's like HID for mobile credentials or outdated legacy hardware, such as HID or Honeywell, that are outside of our control. Instead we took an "Apple-like" approach to the industry and built a better system front to end.

Is the system end-to-end encrypted?

Because Kisi controls the entire stack of the access control system, communication in each step is documented and encrypted on standard cyber security protocols. If you look around, we might be one of the few providers that can answer the question about security documentation easier and more thoroughly than others.

How can I remotely manage and monitor the system?

The Kisi Dashboard is built to manage all your Kisi places from one dashboard. No special configuration is required, just start with your first location and expand over time or standardize access security across all your locations with one seamless setup.

What happens when internet or power goes out?

In any installation, Kisi is installed with an analog backup in place to prevent the worst. For cases when the power goes out and your building doesn't have a backup generator already, the system can be equipped with a backup power supply to keep doors in a certain condition. The ultimate analog backup is often a key switch or pin pad.

For more support, our portal can be found here:

Support

Or contact us directly:
support@getkisi.com
(+1) 646 663 4880