genea

eBook

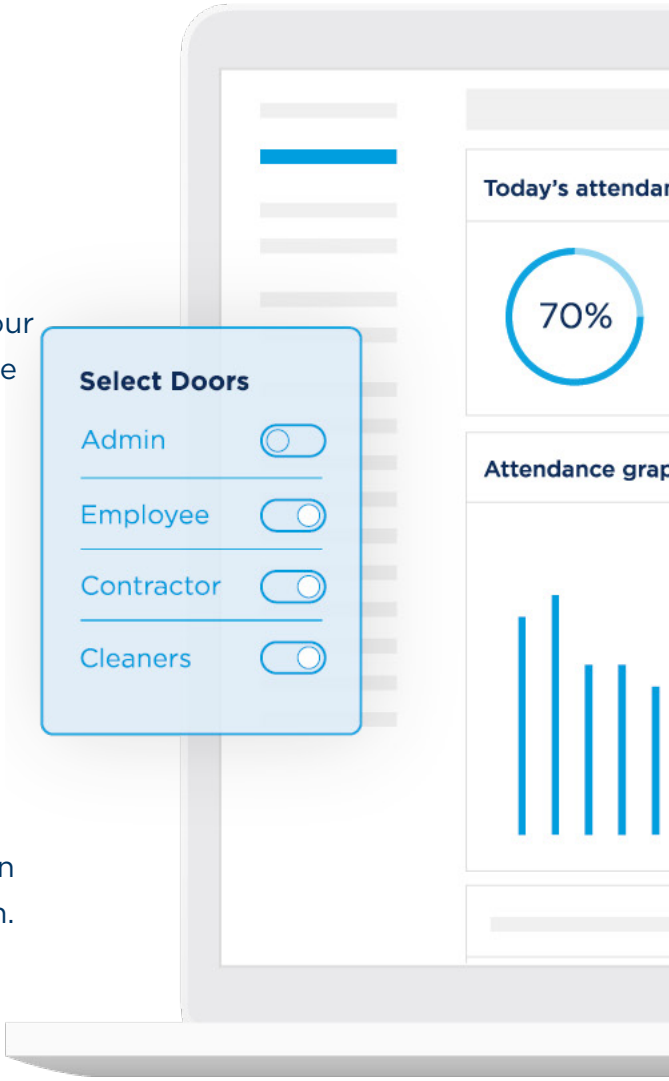
Getting Started With

Physical Access Control

GETTING STARTED

PURPOSE OF THIS GUIDE

Installing and evaluating a new access control system can be stressful. There is a lot to consider when upgrading your current system, and even more so when you're starting from scratch. It does not matter if you're currently using an old school lock and key or you currently have card readers deployed in your facility, this guide will help you evaluate your current needs and find the perfect solution, regardless of the size of your organization and the requirements you have.



IN THIS E-BOOK, WE WILL ANSWER THE FOLLOWING:

- What is physical access control?
- What hardware components are required?
- Is my office already equipped?
- How do I replace my current keycard system?

The purpose of this book is to familiarize you with the ins and outs of physical access control and how your facility can benefit from the increased security of a mobile-first solution. This is true whether you currently have an access control system or are reevaluating your current security needs.

Looking for an all-in-one security solution?

Contact us to learn how Genea can automate your office security and visitor management systems in one easy-to-use portal.

What is Physical Access Control?

THE BASICS

Physical access control specifically refers to restricting the ability to enter a property, building or a room to authorized users only. For our purposes, an authorized user is someone who has permission to enter a restricted area with some credential.

Historically, mechanical locks and physical keys were used to restrict access to secure areas. Unfortunately, physical lock and key setups do not restrict access based on day or time and provide no audit trail of who accessed the space. Physical keys can easily be copied and when lost, often require the entire lock to be re-keyed.

Electronic access control was created to solve the limitations of mechanical locks and keys.

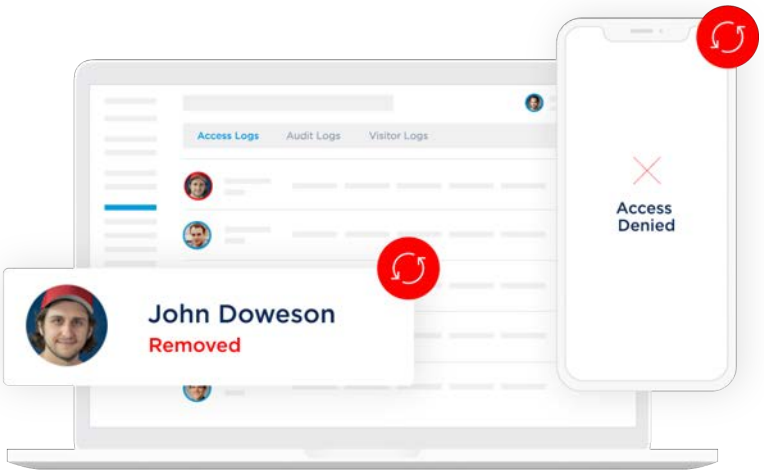
WHAT DOES MODERN PHYSICAL ACCESS CONTROL SECURITY SYSTEM LOOK LIKE?

In modern physical access control, we use electronic door locks and computers to decide who has valid access. The access control system decides who has valid access based on the credential that is being presented.

If a valid credential is presented, the electronic lock will unlock for a specific period of time, allowing authorized users to enter before the electronic lock returns to its default locked state. This unlock time can vary from door to door and system to system.

INVALID CARDHOLDERS

If an invalid cardholder attempts to access the facility, the door will remain locked, and the failed attempt will be recorded. Your system will not only tell you that access has been denied, but it will also give you a reason.



Reasons for Denied Access

INVALID CARD/PIN

The key you have was not recognized by the access control system

NO DOOR ACCESS

You have a valid key but you are trying to use it outside of the timeframe in which you are allowed access

Your access control system can also monitor if a door is being held open for a specific period of time, or if someone has forced a door open.

Piedmont Entry Door	Forced Alarm	Mar 12, 3:19:15 PM

Instead of using a physical lock and key, physical access control utilizes readers and proximity credentials such as key cards or key fobs. There are many different types of credentials that utilize many different types of technology.

TYPES OF KEYS

In electronic acccess control, a credential is your key. These keys come in many different shapes and sizes. They can be physical objects such as key cards, key fob, transmitters, or RFID bracelets. With Genea, these keys can include your phone or smartwatch. More and more, keys can even be part of your body, such as your fingerprint or iris.

WEARABLES

MOBILE DEVICES

KEY CARDS

For the purpose of this e-book, we will use a standard card as our default credential type. When a key card is presented to a card reader, the reader will send that key card's information back to a central controller that will make the decision of whether it is valid or not.

Traditional key cards are simply hardcoded with a number. This number is referred to as a token. If the number is sent to the controller and the controller verifies that the number is a match and associated with an authorized user, the controller will send back a grant command to unlock the door.

The controller that makes these decisions can analyze card swipes very quickly to determine if access should be granted or denied. All of these actions will be logged by your access control system.

TWO-FACTOR AUTHENTICATION (2FA)

A simple card swipe is considered a single factor transaction. This means that an authorized user with a valid credential can share that credential with someone else, and they would have no way of verifying if the intended key holder was in possesion of the key card at the time of entry.

2FA in access control usually consists of a card swipe as the first transaction (something the user has) followed by

- Something the user knows, such as a PIN code or password.
- Something the user is, such as a fingerprint or the use of other biometric feedback.

CREDENTIALS

A credential can be anything that allows one to access a physical facility or a computer-based information system. A credential can be a physical object (such as a key or key card), a piece of knowledge (such as a password or pin code), or a facet of a person's physical being (such as a fingerprint).

In physical access control, the most common credential is a key card. These cards work with many different technologies. Key fobs are also available with the same technology but provide a more compact solution and often allows the holder to attach it to a key ring. Biometric credentials can be fingerprints, iris recognition, hand geometry, and even vocal recognition.

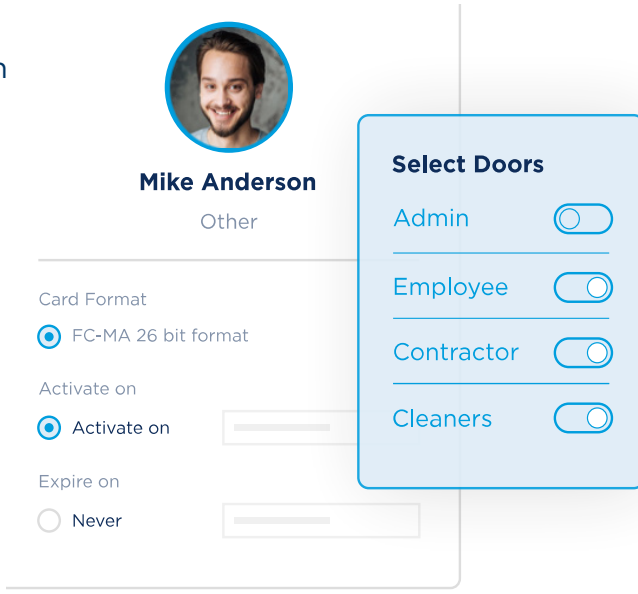
With most modern smartphones being shipped with Bluetooth Low Energy (BLE) and Near Field Communication (NFC), they're increasingly becoming the most efficient way to safely and conveniently serve as an access credential.

BLE TO OPEN DOORS

BLE is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range

NFC TO OPEN DOORS

NFC enabled devices can act as electronic identity documents and key cards. They are intended to provide considerably reduced power consumption and cost



Access Control Security System Components

TYPES OF ENTRY POINTS

Throughout this guide, we will refer to an access point as a door. Keep in mind that a reader can be used to control just about anything including:

Parking Gates **Turnstile** **Elevators**

We will evaluate what access control looks like at an individual door. These components will remain the same throughout your facility with minor changes to the type of lock used for different types of access points.

Physical Access Control Components

A door controlled by electronic access consists of four things:

ELECTRONIC LOCK

This includes mortise locks, magnetic locks, and electronic strikes.

READER

Devices where a credential is presented. They can be set up to read just about anything, including smartphones.

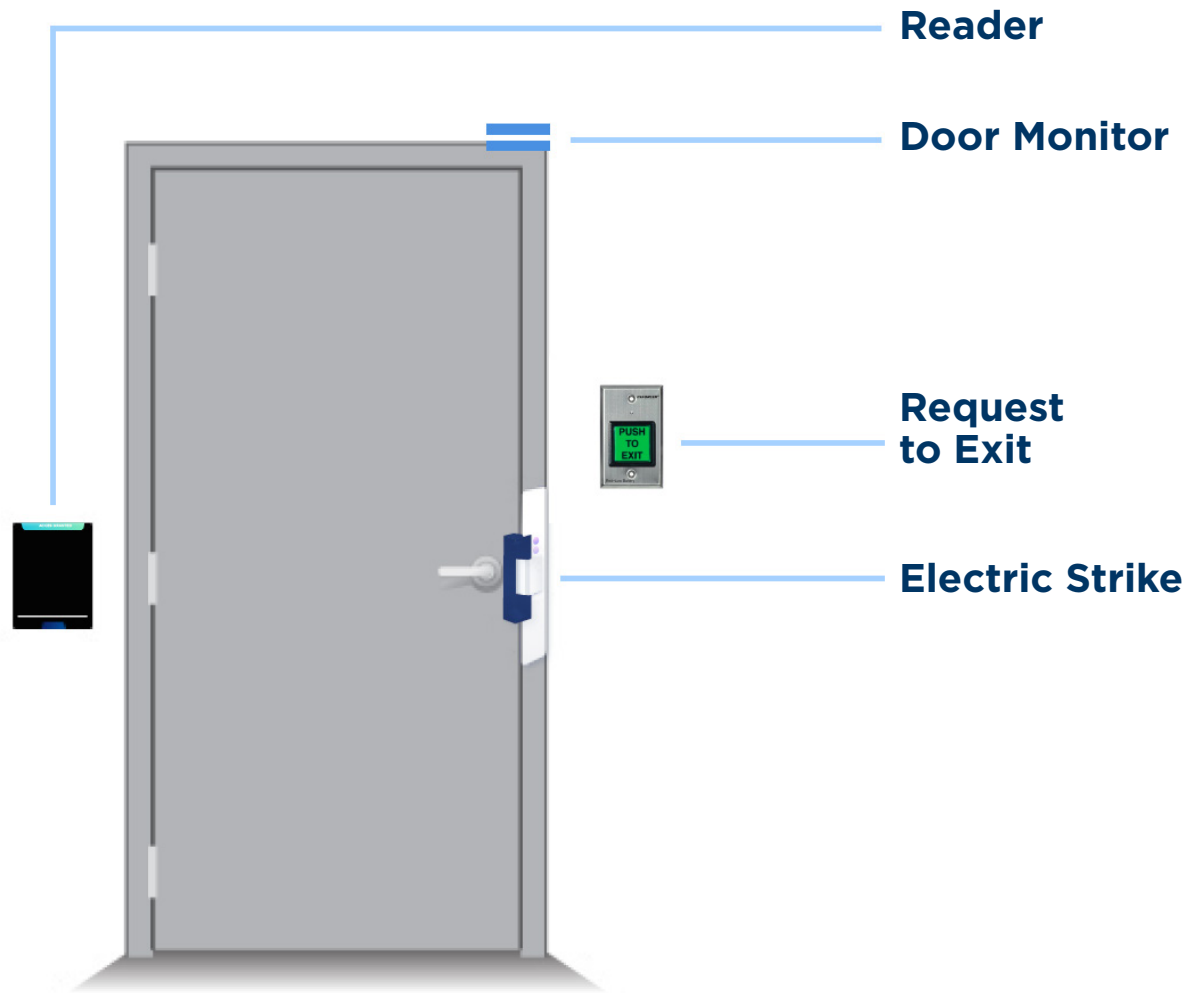
REQUEST TO EXIT BUTTON OR SENSOR

A request to exit button or sensor is used to provide mechanical free egress.

DOOR MONITOR

Magnetic door monitors are placed on the door to track if the door status is open or closed. Door monitors are used to send alerts if a door is being held open or if it has been forced open.

If you have a system in place like this, then you have a huge head start.



Physical Access Control Components (cont.)

In most cases, only entry is controlled by an access control reader. This means that we have a free egress (exiting a locked door without having to present a credential).

In cases where the exit is also controlled, a card reader is needed on the secure side of the door and requires a valid credential to exit. This is usually only used for parking garages.

In most cases, exiting is not controlled and is free. This is acomplished by using a request-to-exit (REX) device. These devices can be a push button on the inside of a door or even a motion sensor that detects movement.

Triggering a motion sensor or pushing a button for exit sends a relay to unlock the door without triggering an alarm. This type of free egress is an important safety feature in case of an emergency.

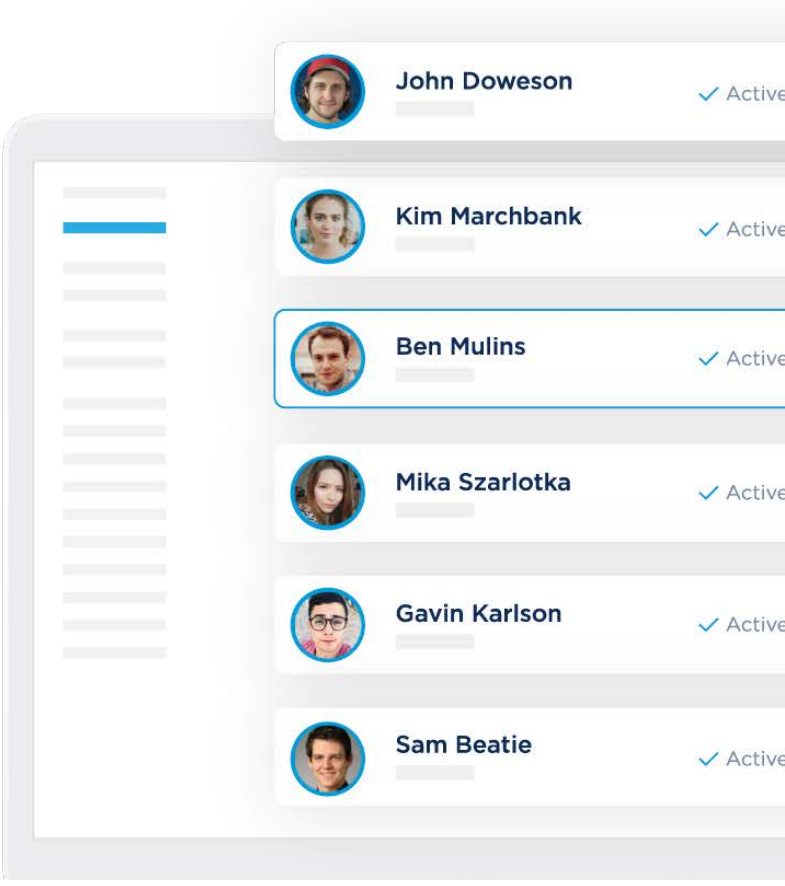
TOPOGRAPHY

When a credential is presented to a reader, the number is sent to a master controller where it is compared to a list of verified numbers. If the scanned credentials number is on the list, the master controller will send a relay to the electronic lock.

Genea stores all of the pertinent access information in two places. It is stored both locally on the master controller, and also in the cloud.

This means that even though your access control system is hosted in the cloud and managed through network connectivity, it will continue to function and operate the same way it usually would when offline.

Additionally, Genea is always installed with a backup power supply so that even if the power to your building goes out, your access control system will continue to function properly.



How to Adopt a New Security System

GETTING STARTED WITH ACCESS CONTROL SECURITY - SET UP AND USE

Moving forward with your access control system adoption shouldn't be a tedious and drawn out process. Whether you've got existing equipment or have a preferred system to install in your new space, in the modern age, setting up your access control system should be painless. And before you waste valuable time ripping holes in walls to install proprietary hardware, know that Genea is the cloud-based platform that can seamlessly integrate within your existing security infrastructure.

While your implementation may differ depending on whether your install is a retrofit or a new install, our process is easy and straightforward.

STEP 1: FREE SITE SURVEY

Before getting started with Genea, we send out an installer to evaluate your site. This helps us give you an appropriate quote for adopting our platform. During the evaluation, feel free to ask our installer any questions you may have about access control and Genea. If you're implementing a new installation, no need to fret. We'll help you choose the best hardware for your facility.

STEP 2: HARDWARE DELIVERED

If you fall into the retrofit category, you can skip this step. For those who are installing new hardware, we'll ship the right equipment based on our site evaluation. We'll also send it to you preconfigured, making installation as pain free as possible.

STEP 3: ASSIGNED A DEDICATED ONBOARDING SPECIALIST

Because we believe modern access control should be as easy as ordering an Uber, we provide you with your own dedicated onboarding specialist. Your Genea representative will verify that you have received the correct hardware, source an installer, walk you though the installation and make sure it's preconfigured to your specifications.

STEP 4: INSTALLATION AND SUPPORT

Once we've agreed on the date of installation, we'll coordinate and send out a certified installer for your Genea system. We know that sometimes you would rather use someone you know and trust, such as a preferred installer or electrician with their low voltage license (for those new installation situations). We can work with them to ensure that everything goes smoothly.

STEP 5: TRAINING AND SUPPORT

Now that you've got Genea all set up and ready to go, we'll provide your team with a full training session on how to use the product and set up your integrations. Our support doesn't stop there. We understand that you may have additional questions after the installation, which is why our support page is chock-full of information. And when in doubt, just reach out to our specialists for those hard to find questions. We're here to help you every step of the way.

About Genea

Genea is the first security management software of its kind. It is built on a state-of-the-art platform, with an emphasis on security and scalability.

Our mission is to help customers like you by providing a cloud-based access control system that's intuitive, open, accountable, and responsive.

With Genea, you can manage credentials, monitor all access activity and assign mobile keys to any device.

See Genea in Action

Genea is the open, cloud-based security platform for the modern growing business. Our API integrations with systems like Okta, Active Directory, and OneLogin allow you to manage your security system from your identity management platform.

Discover how our easy-to-use software can help you manage global access control for all your offices ensuring you're compliant with security policies and regulation.

SCHEDULE A DEMO

genea

eBook

Support

Helpdesk help.getgenea.com
Email support@getgenea.com

Home Office

19100 Von Karman Ave. Suite 550
Irvine, CA 92612