eBook

The Ultimate Access Control Guide to Opening a New Office

Getting Started

Moving into a new office space is exciting. Your company is expanding and growing, and your team is ecstatic to check out their new space. However, setting up a new office is more than just moving your equipment and calling it done.

There's a series of steps between signing the dotted-line on your new lease to opening the doors of your new office space that you must complete. Like any project, undertaking these tasks will test your company's planning capabilities (budgeting, space planning, and data visualization).

While every situation is different (retrofit vs. new build), we'll cover everything you need to know about installing a cloud-based access control system in your new office.

Let's get started.

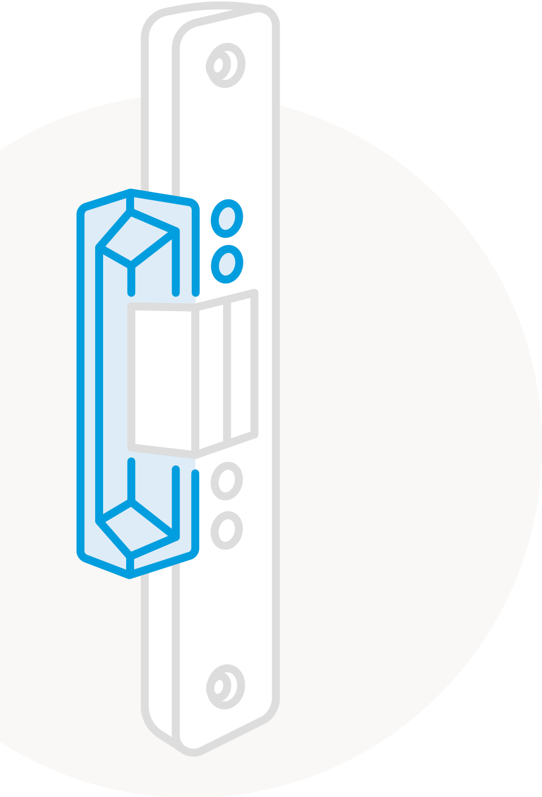
GETTING FAMILIAR WITH ACCESS CONTROL SECURITY One of the most important and least understood parts of physical access control is the installation process. There are good reasons why so few companies exist to do these projects and even fewer that can do them at a truly professional level. The process involves coordinating many moving parts, from hardware and security components to the schedules of personnel, in order to execute installations effectively.

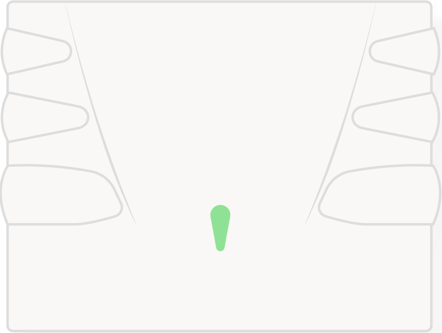
In the early days of Genea, we traveled around the country to help with installations in order to learn this process in painstaking detail. With over three years of managing hundreds of installations, we wanted to give a quick break down of the different components and processes involved with securing your facilities.

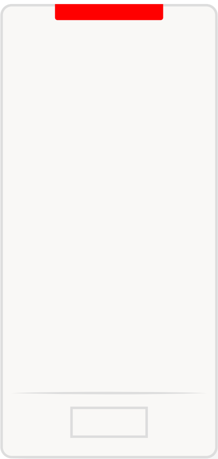
COST EXPECTATIONS

Costs can vary widely based on the city your facility is in, the type of ceilings in the facility, how far the doors are from the IT room and what type of locks are needed for different types of doors. In order to give a general idea of cost, we typically see an average of $650/door in installation costs and another $800/door in hardware (lock, reader, controller, motion sensor).

If you live in a city like New York or San Francisco, you can expect your costs to be about 25-50% higher for labor and components.







The Hardware

In order to understand the process, it’s helpful to get a complete picture of all the hardware involved. Here’s a quick list of the components of a full access control system.

THE MASTER CONTROLLER

This device hosts your local database, bridges your hardware to the cloud, and controls who gets access based on the rules you create.

INTERFACE BOARDS

These devices transport data from the reader to the master controller, and control the lock on the door based on the master controller commands.

THE READER

This is the device on the wall everyone sees. These read your key card or phone’s key number, which the master controller uses to make a decision about whether or not to open the door.

ELECTRONIC LOCKS

Varies between maglocks, door strikes, electronic crash bars, and many other types of hardware that keep your door locked.

ACCESS CONTROL CABLING

These bridge all of the component pieces to transmit data between the readers and controller and transmit electricity between the power supplies and the locks.

POWER SUPPLY

Access control systems require power to function. Your systems power supply keeps the controllers, readers, and locks functioning.

DOOR POSITION SWITCHES

Otherwise known as door monitors, these devices tell you when a door is closed or open.

MOTION SENSORS/REX BUTTONS

These devices allow you to exit a locked door by sensing motion or when someone hits the exit button.

The Process

We'll try to keep this breakdown as short and sweet as humanly possible. Here goes nothing:

1. Before any hardware goes in, it's crucial to get a site inspection done to evaluate how the cables will be run and decide on the hardware that gets installed on the door.

2. During a full office build out, you'll need to run the cables from the room where you will mount all of the door controllers.

3. Next, a locksmith will install the electronic locks on all the doors that will be used to access the facility.

4. Once the cables are run and the locks are in place, a low-voltage technician can connect all of the door components to the controllers and power supplies.

5. Once the hardware is installed, it's time to program your system settings and test some keys. Once you've verified that everything is working correctly, you're all set!

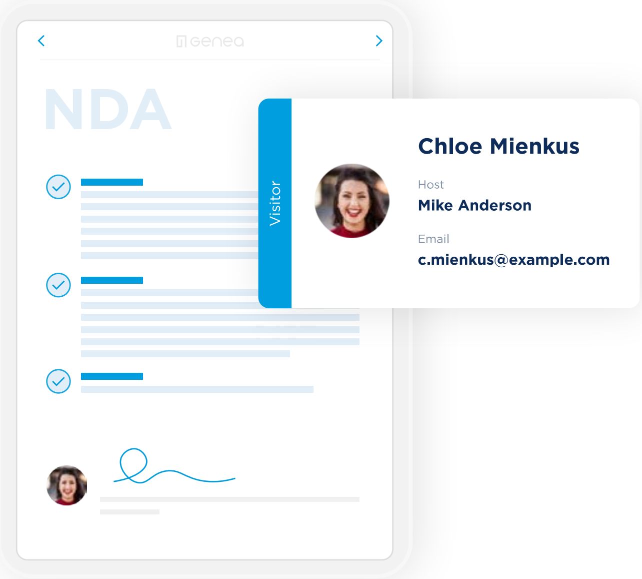
Create and Implement an Access Control Policy

THE IMPORTANCE OF AN ACCESS CONTROL POLICY

Most IT and Facilities teams understand the need to have an access control policy (probably why you're reading this right now). However, a lot of teams are looking for guidance on best practices and how to get buy-in from employees and leadership.

We're going to cover the best practices and give you some tips about how to get employee buy-in to your security policy and get leadership to support and enforce your policies.

Physical access control security systems and policies are critical to protecting employees, a company's IP, trade secrets, and property. These things are the backbone of a company's viability.



Chloe Mienkus

Host
Mike Anderson

Email
c.mienkus@example.com

THE BASICS OF A PHYSICAL SECURITY POLICY

Create a tiered access policy that matches your organizational units, their respective areas of responsibility in the organization, and their physical access to certain areas in your facilities.

Define who should have permanent access and who should have temporary access. It is not always as simple as employees vs. non-employees. Later on, we'll break down that assumption and challenge you to rethink this approach.

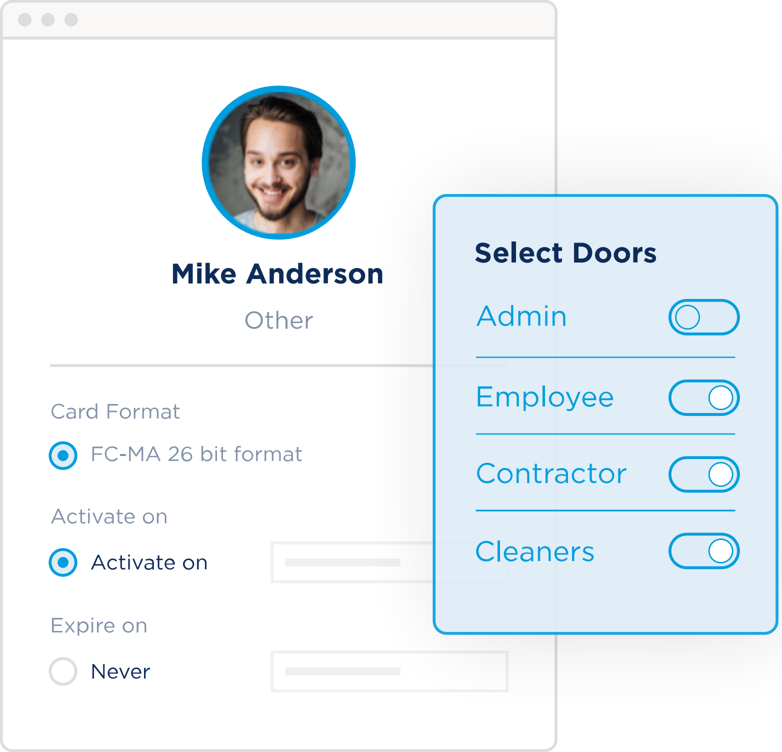
Take the time to invest in employee training and enforcement of your physical security policies. Creating a policy is wonderful, but if it's not adhered to then it is ultimately a waste of time and resources.

Visitor management is more than just a handful of cards and a paper log book.

Consider how these policies and systems fit into your compliance picture?

TIERED ACCESS POLICY

Designing a tiered access policy can be done simply. The basic principle is to match each organizational unit to the doors and areas they explicitly need access to.



Mike Anderson

Other

Card Format

● FC-MA 26 bit format

Activate on

● Activate on

Expire on

○ Never

Select Doors

Admin

Employee

Contractor

Cleaners

IMPORTANT TIPS TO REMEMBER

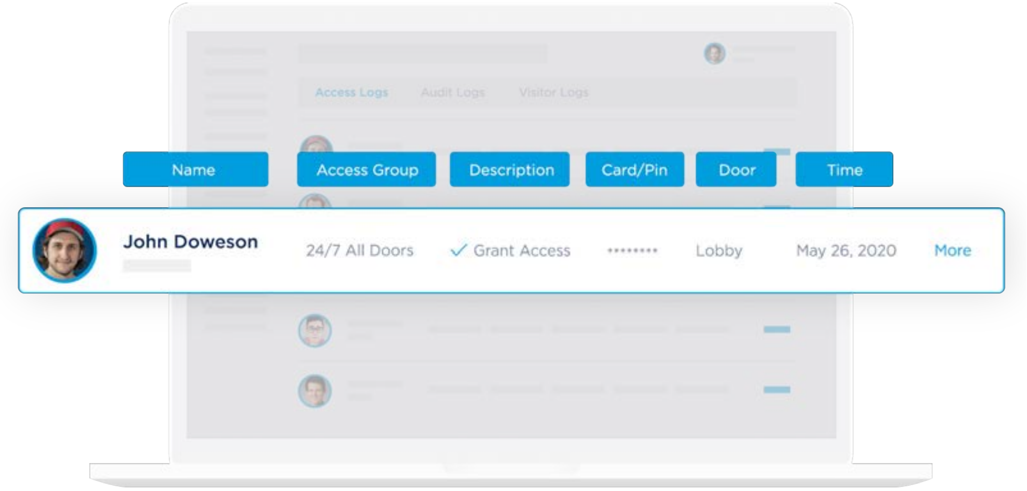
Create a tiered access policy that matches your organizational units, their respective areas of responsibility in the organization, and their physical access to certain areas in your facilities.

It's tempting, but don't let the IT team have blanket access to HR rooms, HIPPA compliant rooms, or other sensitive areas. This will flag auditors and could delay your compliance process.

If you're using an identity management platform like Okta, Ping, or SailPoint. Make sure you're integrating it with your physical access control system and enable automated provisioning. It's important to design provisioning rules that match the organizational unit (OU) in your identity management system to your access groups in your access control system.

Breaking Down Access Groups

Now that we've established our tiered access policy for each OU, it's now time to breakdown the access groups for each OU and develop a policy for permanent vs. non-permanent access to your facilities.



Name	Access Group	Description	Card/Pin	Door	Time	
John Doweson	24/7 All Doors	✓ Grant Access	••••••••	Lobby	May 26, 2020	More

STANDARD EMPLOYEE ACCESS

Often, companies will simply give out credentials with 24/7 access. This might be fine if you're a small company or one that doesn't have significant security requirements. However, since you have read this far, we can assume this means you do not fit that description.

We recommend restricting basic employee access to time frames that allow for early birds and night owls to get their work done when they want, but also restrict access to times when there are more than a handful of individuals in the office. One example might be from 5:45 a.m. to 9:00 p.m.

Why access groups?

Here are a few reasons

- If an employee's credential is stolen or lost, it will prevent access during times when there aren't security personnel or other employees on site.
- Like the buddy system, having more than one person in the office at any given time reduces the likelihood of theft by intruders or even current employees.
- Encourage people to get out of the office! Work is great, but having defined work hours will ensure employees live a balanced lifestyle that reduces burnout.

VISITOR MANAGEMENT

Visitor management can be broken out into a few different types of guests, which all have their own unique use cases. Luckily, now you can manage visitors from the same system as your access control.

Here's a quick breakdown:

CONTRACTORS/AUDITORS

These visitors should be given a dedicated access card that includes their name and their company. These guests typically have a defined time frame when they'll need access. If you know this time frame make sure the credential issued is set to expire! Don't leave it to chance or memory to remember to deactivate their card.

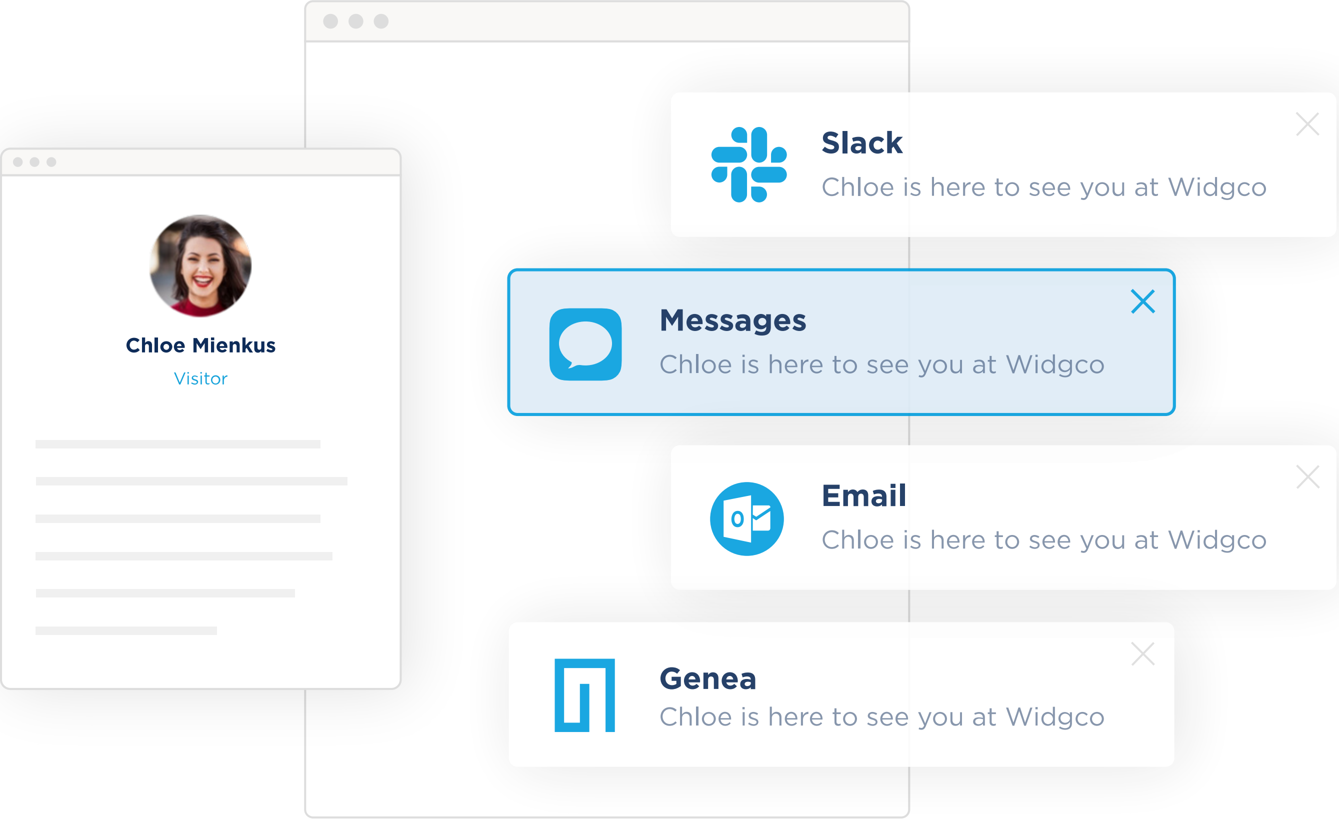
ONE-TIME/SHORT TERM VISITORS

We recommend not giving a credential. Instead, opt for having them go through the facility with the person they're meeting with.

RECURRING VISITORS

These can be vendors like cleaners or caterers that come on a regular schedule. At minimum you'll want to give them a badge that has limited door access and is associated with a specific individual's name. Just having the company name is a recipe for confusion and limits your recourse if an incident occurs.

Have a digital visitor management and logging system. Use a system like our iPad based application to have guests check in and issue them a guest name tag.



Chloe Mienkus
Visitor

Slack
Chloe is here to see you at Widgco

Messages
Chloe is here to see you at Widgco

Email
Chloe is here to see you at Widgco

Genea
Chloe is here to see you at Widgco

PHYSICAL SECURITY POLICY

Having physical security policies and procedures is wonderful, but if they're not being enforced throughout the organization they will fail. One of the hardest, yet most critical aspects of this is employee buy-in from the bottom of the organizational chart to the top.

This is a difficult gap to bridge, but if you engage people from IT and HR to communicate to the entire organization why these policies are for their benefit, you'll get the adoption you're looking for. Ultimately, these policies are in place to protect your employees and the company more broadly. Here are some ways to increase adoption of these policies:

- Have HR incorporate a portion of the employee training and onboarding process to demonstrate your policies and express why they're important.
- Use mobile credentials and enforce Single Sign On (SSO) and two-factor authentication (2FA) for the highest level of physical credential protection.

Tailgating (tail•gat•ing)

Tailgating is when an employee holds the door open for others and is one of the simplest ways for an intruder to bypass your security measures. You should post signs at major entry points to discourage this practice.

ADVICE FOR COMPLIANCE

Now that you've created a physical security policy, it's important to document and host it in a company Wiki. You'll want summarize each aspect of the policy, such as the access group matrix, visitor management policies, where you log your data, who has access to the software system, and more.

If you're using an identity management platform, make sure you integrate SAML SSO and set up automatic provisioning for lifecycle management. This will ensure you close critical failure points and are adhering to your compliance needs.

If you're using a security information and event management (SEIM) tool like SumoLogic or Splunk, port your data and create a dashboard for tracking and logging activity across your suite of facilities.

Integrate Access Control Security and Visitor Management

WHY YOU NEED TWO SYSTEMS

There comes a time in any company's life cycle where IT has
to stop and reevaluate all the tools they're managing. With SaaS taking over every aspect of a company's operations, the need to cleanse has become more frequent.

One way to accomplish this is by consolidating two different products with the same vendor, which can give you a number of benefits like bigger discounts, less systems to manage, and fewer renewal meetings. Trust us, the thought of fewer meetings is as pleasant as meditating on a Saturday at the Presidio.

SIMPLIFYING THE PROCESS

We're on a mission to make managing physical security for the modern enterprise as easy as possible. We launched a beautiful, seamless access control management system that allows customers to automate access provisioning through identity management integrations. We took it further by integrating a visitor management system.

Visitor management should be a natural component of your overall access management system. Our native visitor management app allows you to have one central platform for tracking and managing physical access to all your offices. Whether it's a guest or an employee, we believe that access to your office or facility is better managed on an integrated platform, not to mention the ease of having everything in one place.

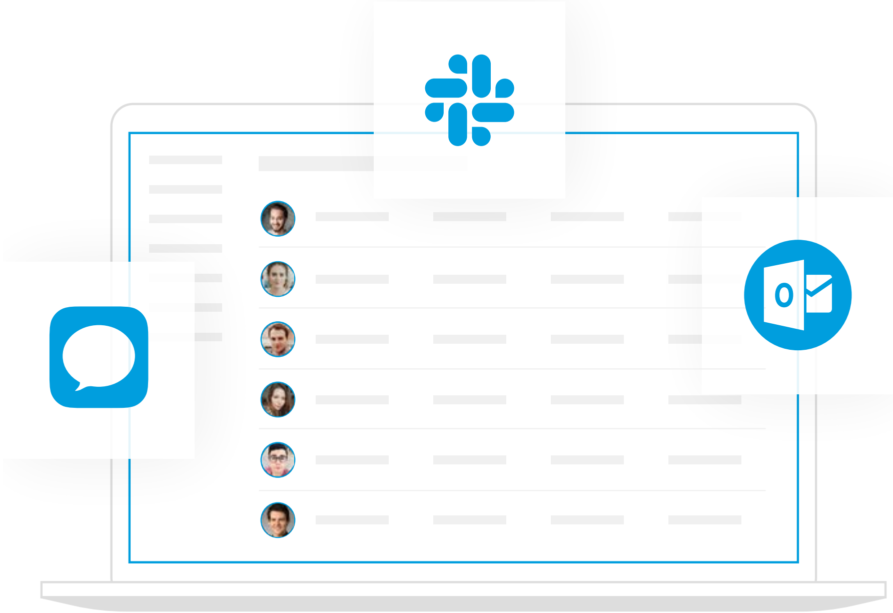
HOW GENEA'S VISITOR MANAGEMENT SYSTEM WORKS

1. Grab an iPad and download the Genea Visitor Management App

2. Pair the iPad with your access control system

3. Set up your sign-in flow

4. Sit back and enjoy the peace of mind of having one less system and vendor to manage



KEY BENEFITS

- Access and Visitor Logs All Under One Roof
- Central User Database
- Saves Money

ABOUT GENEA

Genea is the first access control management software of its kind. It's 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 access control for the modern growing business. Discover how our easy-to-use software can help you manage global security for all your offices and ensure compliance with security policies and regulation. Our API integrations with systems like Okta, Active Directory, and OneLogin allow you to manage your physical access control security system from your identity management platform.

SCHEDULE DEMO

Genea

eBook

Support

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

Home Office

19100 Von Karman Ave. Suite 550
Irvine, CA 92612