ievo

Securing the Retail Industry

Creating a secure and effective system providing the utmost top security measures is a prime target for the retail industry to comply with store security, safety and loss prevention guidelines. With areas containing high value assets, and outlets and storage facilities with a high volume of footfall, it is important that the most advanced systems are employed to provide protection. **ievo** Ltd have a proven track record in providing reliable and efficient biometric solutions that enhance access control for a higher level of security.

SECURING YOUR ENVIRONMENT

Many tech savvy retailers look to adopt an efficient and simple time and attendance protocol as part of its access control security infrastructure. Systems not only control physical access, but can provide time and attendance monitoring to outlets, high value asset storage rooms, or staff areas, to help keep an accurate record of who is where and when.

REMOVING RISKS

One if the issues retailers face when using security systems reliant on swipe cards, fobs or PIN passwords, is the sharing of these secondary credentials between staff members. The dangers of using such a system are that it can leave your security measures vulnerable, and can be compromised further should these credentials be in the procession of non-staff members.

ievo biometric solutions removes these issues and concerns due to the very nature of how the data is captured. **ievo** authentication devices utilise the biometric data forming an individual's fingerprint, once a system is installed only users with a registered fingerprint template will be granted access through protected entry points.

The data captured at the time of scanning for identification can also provide your access control system, with time and date data, meaning you will know who accessed what and when. This data can be used to create highly accurate and reliable attendance monitoring for increased health and safety and fire records.

Installing **ievo** biometric readers as part of your security system can help safeguard high value assets or inventory, only those registered for authentication and with set access permissions will be permitted. There is no danger of access 'keys' being shared, lost or reproduced. This is ideal for storage areas or warehouse facilities with high value attachments.

COST SAVING

An **ievo** integrated biometric access control system can help to reduce costs to your security infrastructure; simple installations means less on-site for engineers, the modular design of **ievo** systems makes for easy maintenance, integrated systems makes for more practical and functional solutions. The use of time and attendance integration can aid HR, health and safety records and other building services.
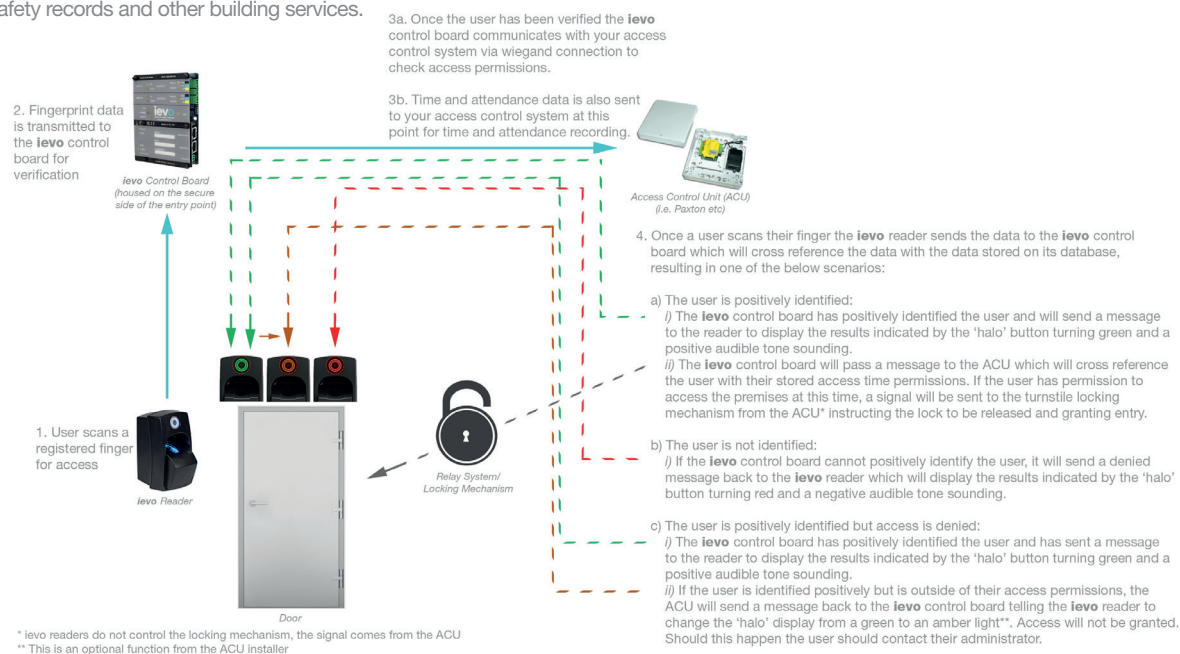
DEPENDABLE RELIABILITY

Access levels are an incredibly important way of monitoring staff within a secured premises. Firstly, the term 'access level' refers to allowing certain people access in one or multiple areas of the site, depending on which doors are secured. You can mix and match access levels within an **ievo** system via your access control infrastructure. For example, if you have two **ievo** fingerprint readers on site, one for a staff entry point and the other on a product storeroom, you can restrict users from gaining entry to the storeroom, while allowing all staff members access to the main door.

In addition, if an incident did occur on site, i.e. theft or vandalism, you would be able to check the access control unit logs, showing you exactly who scanned in and at what time. This gives you maximum authority over your premises and the contents within.

TECHNOLOGY THAT PROMISES PROTECTION

The flexibility of **ievo** products means that any site, whether big or small, can be securely protected. From a single door with access control, to a site with multiple doors, car park barriers and rotating doors/turnstiles; or a small outlet with low number of employees to a warehouse facilities with a large workforce, the **ievo** range can be tailored to your requirements.

ievo solution integrate with a wide selection of popular access control systems including; Paxton, PAC Stanley, Honeywell, ACT and Nortech. For more information please speak to a member of our support team.

2. Fingerprint data is transmitted to the **ievo** control board for verification

ievo Control Board (housed on the secure side of the entry point)

1. User scans a registered finger for access

ievo Reader

Door

Relay System/ Locking Mechanism

3a. Once the user has been verified the **ievo** control board communicates with your access control system via wiegand connection to check access permissions.

3b. Time and attendance data is also sent to your access control system at this point for time and attendance recording.

Access Control Unit (ACU) (i.e. Paxton etc)

4. Once a user scans their finger the **ievo** reader sends the data to the **ievo** control board which will cross reference the data with the data stored on its database, resulting in one of the below scenarios:

a) The user is positively identified:
 i) The **ievo** control board has positively identified the user and will send a message to the reader to display the results indicated by the 'halo' button turning green and a positive audible tone sounding.
 ii) The **ievo** control board will pass a message to the ACU which will cross reference the user with their stored access time permissions. If the user has permission to access the premises at this time, a signal will be sent to the turnstile locking mechanism from the ACU* instructing the lock to be released and granting entry.

b) The user is not identified:
 i) If the **ievo** control board cannot positively identify the user, it will send a denied message back to the **ievo** reader which will display the results indicated by the 'halo' button turning red and a negative audible tone sounding.

c) The user is positively identified but access is denied:
 i) The **ievo** control board has positively identified the user and has sent a message to the reader to display the results indicated by the 'halo' button turning green and a positive audible tone sounding.
 ii) If the user is identified positively but is outside of their access permissions, the ACU will send a message back to the **ievo** control board telling the **ievo** reader to change the 'halo' display from a green to an amber light**. Access will not be granted. Should this happen the user should contact their administrator.

* ievo readers do not control the locking mechanism, the signal comes from the ACU
** This is an optional function from the ACU installer

RELIABLE. BIOMETRIC. SOLUTIONS.

KEY BENEFITS OF IEVO SYSTEMS

- Safe and secure environment for your employees
- Improved fire and health & safety records
- Additional layer of security
- Cost effective
- Integrated system to work with your infrastructure
- Software integration opportunities available
- Future proof design - for any future upgrading or additional development of your security system
- Full customisable and serviceable up to and after the point of sale
- Customisable colours to discreetly blend into your environments.

ievo Ltd is a leading design and manufacturer of biometric fingerprint readers. Working with installers and integrators, **ievo** Ltd have a proven track record securing retailers worldwide.

For case studies or further information, please contact our support team:
info@ievoreader.com
Tel: 0845 643 6632 / +44 (0) 191 296 3623
or visit:
www.ievoreader.com