EyeLock Technology FAQ

Version 2.1

July 2021

Our vision for your secure world.

EyeLock, LLC.
321 West 44th Street, Suite 702
New York, NY 10036
USA
Phone: (855) EYELOCK / +1 855-393-5625
Contact us: sales@eyelock.com or support@eyelock.com
Download the software at http://help.eyelock.com/
License the software at https://license.eyelock.com

Table of Contents

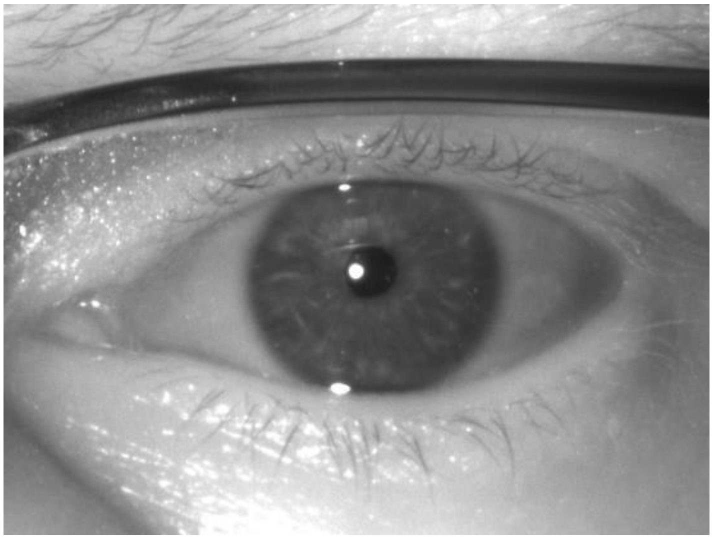
1. Basics: How Iris Recognition Works

What is the history of iris recognition?

The uniqueness of iris as a human identification feature has been known since mid-20th century. In the mid-90s it was formulated into a computer algorithm, evolutions of which are still in use to this day. The standardization efforts in around 2010 solidly put iris recognition on the map as one of three main biometric modalities, along with fingerprint and facial recognition. It has since been tested on tens of millions of people around the world. Modern algorithms perform sub-second matching across millions of records.

How does iris recognition work?

The process starts by taking a high-resolution photograph of the iris, like the example shown below. The software subsequently finds where the iris, pupil and eyelids are located in the photographic image, then removes all areas but the iris pattern, further massages it, and applies a special mathematical transformation to convert it into a biometric template. The iris biometric template, several hundred bytes in size, is the only extract of the image needed for biometric matching. The iris matching algorithm compares the templates to other templates stored in a database, looking for a match.



Example of an iris image.

What makes irises so unique?

The iris pattern is random and formed before birth. The pattern structure is unique to all individuals. Even identical twins have distinctly different iris patterns.

Do iris images change over the lifetime?

Generally, no. There were multiple scientific studies challenging this statement, and the current consensus is that the iris pattern remains unchanged, within the accuracy required for biometric identification, throughout the lifetime. Out of the 3 main modalities, face, iris and fingerprints, the iris recognition is the most stable biometric technology.

Is the retina scanning the same as iris scanning?

Not at all. Iris scanning uses photographs of the eye, usually with near-IR light. It may not even require additional lighting if the ambient lighting is sufficient. Retina scanning views the vein pattern on the back of the eye. It has not been used commercially for decades. There are no retina scanners on the market at present.

How much more accurate is iris scanning than facial recognition?

The accuracy of iris technology is orders of magnitude higher than the accuracy of facial recognition. Unlike the facial appearance, the appearance of iris pattern does not change over time, it does not get occluded by facial masks and protective shields, and the irises of twins and siblings are different.

Are contact lenses OK to wear?

Yes. Contacts are not a problem because they do not substantially occlude the iris image. However, patterned contact lenses, such as Halloween cat eyes, will not work.

Can iris recognition be used if people wear facial masks and shields?

Yes. Iris recognition works if at least one eye is visible.

How do eye diseases affect iris capture?

Usually, they do not. The common cataract surgery, where the lens of the eye is replaced, if successful, does not change the iris appearance and thus iris recognition performance.

Is iris recognition a surveillance technology?

Not really. Iris recognition is a biometric technology, and the iris template is a type of PII (Personally Identifiable Information). However, unlike facial recognition, even though intrinsically more accurate, it cannot be deployed as a surveillance technology because the iris capture range is short, not exceeding about three feet, and the users are required to cooperate by actively looking at the camera. There have been several experimental systems developed a decade ago that would capture irises at fifteen or so feet, but they turned out refrigerator-sized and still required active user participation. In fact, one of them did have a refrigerator inside to keep the massive bank of electronics from overheating!

2. Core Iris Recognition Technology

Are there known demographic biases in iris capture?

Unlike most common types of facial recognition, the iris recognition has generally been proven to work equally well for all types of people regardless of gender or race. A recent DHS S&T Maryland Test Facility experiment, as an example, shows no correlation between the accuracy of iris recognition and demographic factors. Biometric matching between twins and siblings is statistically the same as the matching of completely random people in the world.

Is the iris capture process standardized?

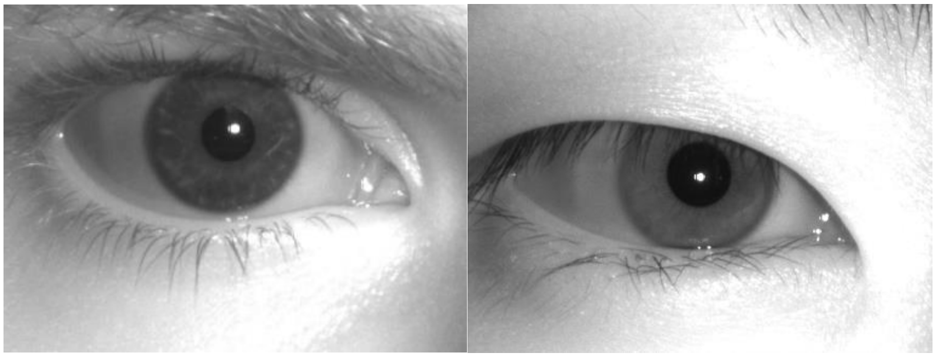
Yes. Iris, face and fingerprint recognition are the three main biometric modalities which are standardized by NIST and ISO and investigated from multiple perspectives. The iris capture process is standardized via ISO Standard 29794-6 to ensure interoperability of iris images captured by different cameras with different matching algorithms. The iris template is not standardized; different vendors use their own proprietary templates.

What is the accuracy of iris recognition devices?

Iris is the most accurate biometric modality, and it is second only to the DNA recognition in terms of its unique identification signal. EyeLock devices are normally configured to operate at 1:1.5 million false acceptance rates.

Why is infrared illumination used?

Even though the features of human irises are visible in normal white light, near-infrared (NIR) illumination helps equalize the brightness of irises. Dark brown and bright blue eyes appear almost the same in the IR light, thus simplifying the capture process. The physical process is that the melanin, which makes the eyes appear dark in visible light, is transparent in infrared lighting.



Visual appearance of blue-eyed and dark brown-eyed persons when photographed in infrared.

Why are there LED lights on both sides of the camera?

Most EyeLock devices provide infrared illumination from the left and the right sides of the camera. Although only one side is required for iris capture, using two facilitates the capture of good images if the person is wearing glasses. The glasses may cause direct reflection of the LED light onto the camera, locally saturating the image; shifting the illumination to the other side of the camera avoids this problem.

Why are the IR LEDs located several inches away from the camera?

Placing the LEDs several inches away from the camera dramatically reduces the red-eye effect, similar to what happens in casual photography. Red-eye occurs when the LED illumination passes through the pupil and illuminates the retina, reducing contrast between the pupil and the iris, possibly confusing the segmentation algorithm. The ISO Standard for iris capture requires high contrast between the iris and pupil areas of the image.

Do the devices capture through sunglasses?

Yes, since most sunglasses are transparent in infrared. Some sunglasses may present an issue if they are very dark and not transparent to IR.

Can iris recognition be spoofed?

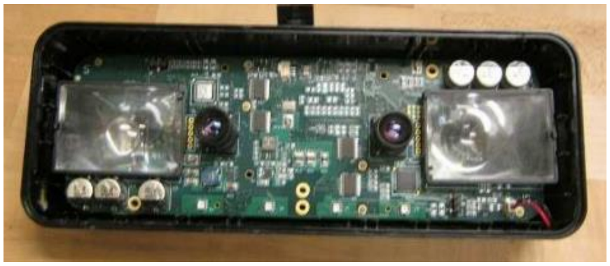
As seen in the Minority Reports sci-fi movie, any type of biometrics can be spoofed, but spoofing of irises is very difficult. We do not advertise the anti-spoofing mechanism we utilize. But rest assured, showing a photograph of a person to an iris camera will not open a door!

3. EyeLock Devices

nano EXT device installed outdoors.

What's inside EyeLock devices?

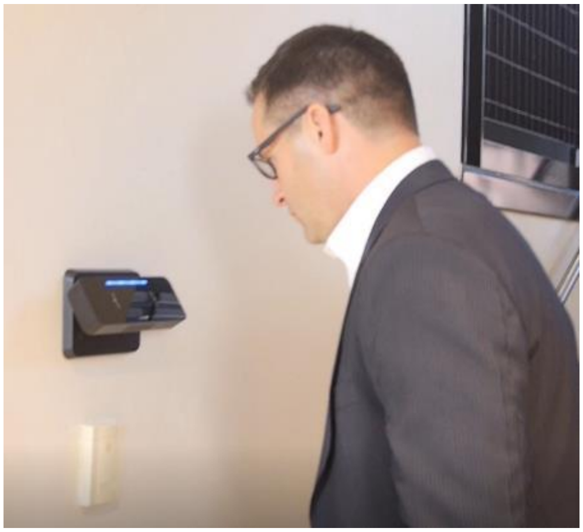
All EyeLock devices have pulsed IR LEDs, one or multiple infrared-sensitive CMOS cameras, an embedded microcomputer, and power/pinout circuitry. The rest varies by device: some may have touch print LCD, RGB indicator LEDs, USB ports, POE, as well as mechanical movement components.



Inside of nano NXT camera are 2 cameras and IR LED illuminators.

Is iris scanning safe?

Yes. Iris recognition products utilize LED illumination. No lasers are used. All EyeLock products are tested by third parties for compliance as per IEC 62471 PHOTOBIOLOGICAL SAFETY OF LAMPS AND LAMP SYSTEMS - Edition 1 - Issue Date 2006-07 and CENELEC EN 62471 PHOTOBIOLOGICAL SAFETY OF LAMPS AND LAMP SYSTEMS - Issue Date 2008-09 standards. EyeLock devices are classified as "IEC 62471 EXEMPT RISK GROUP", meaning eye safe with no safety labeling required. Even the most lightemitting EyeLock product, nano EXT, emits light at only a small fraction of that allowed by the "EXEMPT" category power.



Typical nano NXT installation.

What are the advantages of dual eye capture?

All EyeLock devices provide dual eye capture, meaning that both eyes are photographed at the same time. Simultaneous capture of both eyes in one snapshot significantly reduces the failure-to-capture events, especially when the person is wearing glasses.

Are both eyes required?

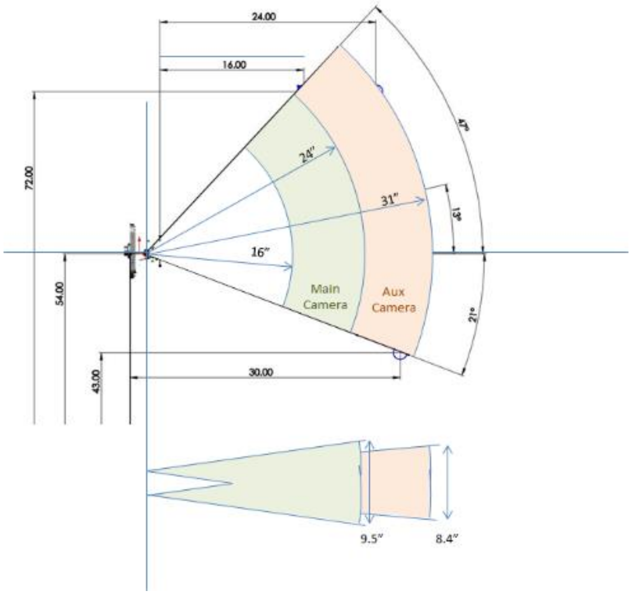
Generally, no. A single eye is sufficient for reliable recognition. Enrolling both eyes is a good idea since it reduces failure-to-capture rates during recognition.

How large can the iris database be?

EyeLock access control devices support in-device databases as large as 20,000 records (persons). Larger databases can be supported via backend matching at the EyeLock EIS server. By far the largest iris database in the world is operated by the government of India; it contains about 1.2 billion records.

At what distance can iris capture occur?

Depends on device used. The EXT captures irises located anywhere from 16" to 32" from the device, possibly the largest capture volume in the industry. A built-in privacy feature of iris recognition is that the capture cannot occur at distances over about three feet. People need to actively look at the camera to be captured.



Capture volume diagram of nano EXT camera.

Do EyeLock devices capture facial images?

Some EyeLock devices capture facial images that can be used for biometric matching or for event logs.

Does EyeLock provide device SDKs?

Yes. Several device SDKs and web APIs are available depending on the application.

Can the devices collect biometric information for subsequent matching via 3rd party backend systems?

Yes. Iris and face images from EyeLock cameras are interoperable. Device SDKs for integration are available.

Can EyeLock devices be used for Time and Attendance (T&A) applications?

Yes. If fact, it's a common application of our technology. The EyeLock backend platform records all time clock events in the EIS (EyeLock Identity Suite) database which can be integrated with accounting and other systems.

nano NXT devices used for T&A at an industrial plant.

4. Access Control Solution

Are all EyeLock devices interoperable?

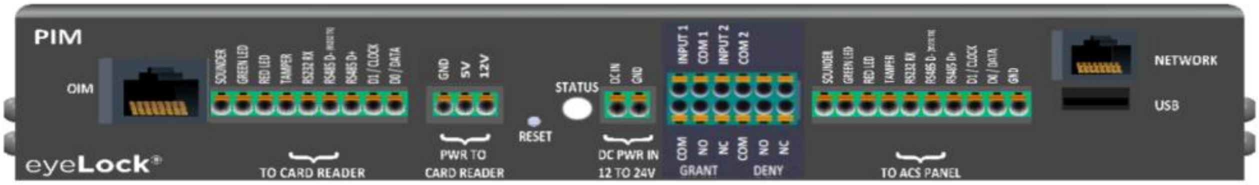
Yes. All devices use the same type of template and have the same database structure. They can connect to the same EyeLock backend integration platform EIS in any combination.

Are EyeLock devices interoperable with other iris devices on the market?

Only in the sense of the images they capture and the matching algorithm. In an access control solution, the interoperability is lost since proprietary data structures and APIs are in play.

What are the physical ports of EyeLock access control devices?

There is a range. Generally, all devices have Wiegand In/Out ports. NXT and EXT devices also support OSDP. All devices have at least one door relay. The communication to the devices is via Ethernet, though USB may be used too.



Ports exposed on nano EXT device.

Do I have to have our Access Control System (ACS) integrated with EyeLock?

No. However, the benefit of integration is that the operator does not need to type in card numbers and manage cardholders in two separate systems.

Do I have to have an Access Control System (ACS) software?

No. EyeLock EIS software can serve as a rudimentary access control system. However, it lacks advanced features which are present in many commercial ACS software solutions.

How do I connect card readers?

External Wiegand/ OSDP card readers can be connected to any of the EyeLock access control devices. iXT device has a built-in card reader that supports only 13.56 MHz cards at present.

How do I provide power to EyeLock devices?

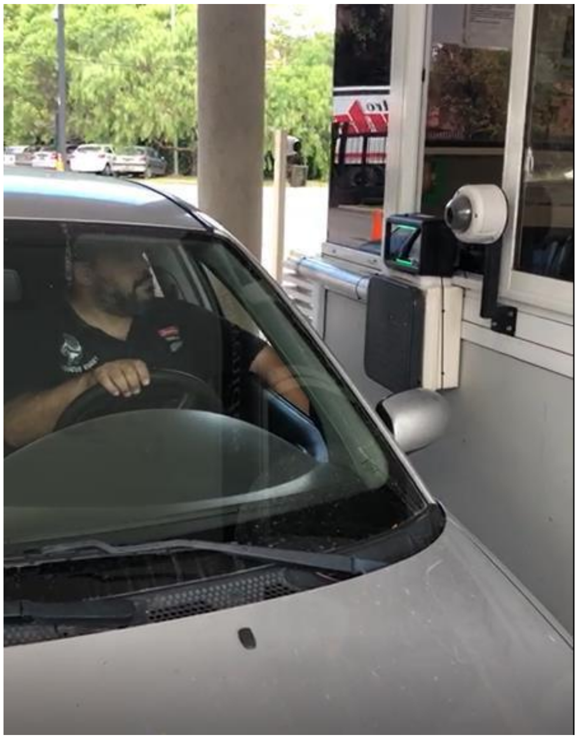
Nano NXT is a POE device. Nano EXT and iXT require an external power supply. External POE+ adapter may be to power with iXT. myris is a USB device.

What devices can be used for the enrollment?

Any, with exception of nano EXT. Ergonomic and system architecture factors determine the preferred device for the enrollment operation.

Which devices can be used outdoors?

Nano EXT. It is IP67/ IK10 tested, has a separate secure-side electronics module and its optics are designed for operating in very brightly lit areas.



nano EXT device installed outdoors at a car port.

What card types are supported?

EyeLock system supports standard and custom cards. A unique feature of the EyeLock solution is that it can support multiple card types at the same time. For example, a facility can operate with legacy Wigand 26A and newer issue Corporate 1000 cards, in the same system.

Which iris scanners have a body temperature option?

The iXT has a body temperature accessory called iTEMP.

iXT device with iTEMP accessory installed.

Can EyeLock devices be used in turnstiles?

Yes, using Wiegand/OSDP or the dry relay contact of the turnstiles.

Nano NXT devices used for commercial office access.

What is a Portable Template?

In the Portable Template solution, the template is provisioned to a dedicated access card or a mobile phone app at the time of enrollment. During the authentication process, the template is read from the card or the phone and biometrically matched to the live capture images. If matched, then the device sends Weigand/OSDP ID of the user for authorization by the control panel. In the Portable Template solution, the biometric data always resides with the user; it is never uploaded into the database. The users “own” their biometric data, which may help mitigate their privacy concerns. Note that the solution requires smart cards and smart card readers specified by EyeLock.

5. System IT

What cybersecurity mechanisms are utilized in the EyeLock solutions?

Multiple, and at different levels.

- Templates are AES256 encrypted. In general, the templates are proprietary to EyeLock.
- All passwords are encrypted in the database, including ACS integration passwords.
- Device communication is via TLS AES256 encrypted channel.
- The software and firmware are scanned for vulnerabilities, with found vulnerabilities addressed before release.

Can EyeLock devices be used on an IPv6 network?

nano EXT and nano NXT devices and EIS can operate on IPv6 networks.

Does EyeLock provide a generic iris recognition SDK?

EyeLock does not provide internal iris matching SDK as a product because EyeLock SDKs are designed with higher-level integration in mind. Also, the internal EyeLock SDK takes advantage of certain device hardware features which are unique to EyeLock to achieve highest accuracy.

Can EyeLock system be used for logical access such as computer login?

Yes. We have several means of integration. The EIS database can support username/password in addition to card numbers, and both can be exposed via integration, which allows creating mixed systems where, for example, some recognition devices are used for opening doors, while others are for accessing industrial equipment.