****

**FAQ about Iris Biometrics**

**Can Iris Biometrics reduce log-in time?**

Yes. Iris Matches take approximately 1 - 2 seconds. Integral's automated logins take between 500ms and 1 second (depending on the integrated application.)

**Can Iris Biometrics reduce password failures?**

Iris based logins are consistent and reliable. Password failures should be completely eliminated.

**Can Iris Biometrics prevent human error?**

Yes, by reliably recognizing a user and providing the correct login credentials every time, the Iris Biometric solution eliminates human error from the Login process. Human error can have a small impact on login times and reliability of the Biometric solution in some ways. If the user does not use the sensor properly, they can fail a match or take longer than normal to match. Once trained to hold the sensor properly or if mounted to look into it properly, which is very easy, then the user can get consistent, reliable performance.

**Can Iris Biometrics help with cost saving?**

Iris Logins take .75 to 2 seconds (depending on network performance for remote sites) with trained users. By eliminating failed logins and lockouts and completing logins consistently 10 - 15 seconds faster than a user can do manually, a Biometric solution delivers significant time savings for a typical user who logs in 30 to 120 times a day. Biometric solutions on average can save 100 hours a year per user. For systems that use Touch screens for logins, the savings are even higher. Also, Iris Biometric solutions eliminate password resets which eliminate the personnel cost for password resets along with the related delays. By eliminating glove removal and replacement to use fingerprint devices, the Iris solution saves more time and cost. By potentially increasing the quality checks and measurements in the shop floor workflows due to leveraging faster and more reliable and easier logins, there is an opportunity to increase quality of the product which will reduce downstream costs related to lower quality product.

**Can Non-Fingerprint Biometrics eliminate the amount of password retries?**

Yes. It will login reliably every time the user matches**.**

**Does Iris Biometrics speed up Log in process?**

Yes, It will login reliably every time the user matches and will take 1-3 seconds to complete each time.

**Can Iris Biometrics help with the efficiency of operations?**

Integral's Iris biometric solution has been shown to Increase productive output of shop floor systems by 7%. Our customers have measured 10X and 16X faster logins.

**Can Iris Biometrics help with shop floor operator satisfaction?**

People HATE Passwords. Passwords stop them from getting their work done. They make them feel stupid when they don't remember them. They resent not being trusted and are reminded of that every time they login. Eliminating these stressors is deeply appreciated and removes a regular irritant from the typical worker's day. Also, most system implementations in the factory are designed to make the product faster, better, and cheaper, but usually there is extra, more complicated work for the user to achieve these goals. By implementing Iris biometrics, you implement a system that achieves all the business goals while making work easier for the worker as well. This is rarely achieved and end users deeply appreciate receiving a system that finally makes their work easier. Additionally, as a human being, it is satisfying to be recognized. How often do we use technology and think, why doesn't this device know me by now? I use it all the time. With an Iris biometric, the user has a human experience of looking at the machine and having it finally see them and know them and do something to help them. This is inherently satisfying.

**Is it easy to use Iris Biometrics?**

Yes! Glance at the mirror on the device and then look away. Done… No typing, no ID's to remember, no mistakes. That is a big, Yes.

**Is the maintenance of Iris Biometrics devices easy?**

Yes. Swab them down with 70% alcohol solution from time to time. Keeping them on a mount minimizes touching and dropping and the need to clean, so maintenance should be rather easy.

**Can you save time switching from systems (MES, Control Systems etc.) by using Iris Biometrics?**

The time saved here is achieved by shortening the login times and making them consistent. The Integral application can recognize numerous applications and log into them or do eSignatures without any user action as long as the systems have been integrated..

**Can Iris Biometrics increase usability?**

Yes. It will login reliably every time the user matches. They just glance at the sensor and they are done. Touch screen systems and shop floor HMIs benefit the most from this solution due to how slowly users interact with touch screen keyboards. A kaizen study done at a major Pharmaceutical company found that our fingerprint solution is 16 times faster than a manual touch screen login.

**Can Non-Fingerprint Biometrics prevent shared passwords?**

Yes, Iris and fingerprint biometrics ensure that only the matched user can login. The Integral system currently checks for unique usernames when enrolling users for an application and recording their login credentials. Users are blocked from having the same login ID for a specific application. The Integral system does not let users change their username once provisioned by an Admin, so there is no way for a user to input another user's credentials to be used with their biometric match.

 **Can Iris Biometrics help with compliance?**

The Integral solution ensures compliance by guaranteeing that the operator who signs on something biometrically is always the person associated with the logged credentials. Iris match reliability of 1 in 2.25 trillion (with 2 eyes) essentially makes it impossible to document the wrong person.

**Can Non-Fingerprint Biometrics be used in an environment with gloves?**

Yes, Iris biometrics have small cameras and lights that must see the user's eyes. Gloves have no impact on Iris biometric matching.

**Can Iris Biometrics be used with safety glasses?**

Iris biometrics can match user's eyes through safety glasses, goggles, and other face protection. Integral’s Myris’s Iris scanning technology works with users wearing clear contacts, plain colored contacts, glasses and safety goggles.Cataract surgery and/or other lens-replacement surgeries do not affect the iris in anyway nor do they prevent the technology from working effectively.

**Can Iris Biometrics be used in an area where users are gowned up?**

Yes, the Iris sensor can be used in an area where users are fully gowned. The sensor must be able to see the user's eyes. It requires no additional visibility. Since operators must be able to see in order to work, it follows that their eyes will be visible when they are gowned and masked at any level of gowning.

**Is there less risk of contamination with Iris Biometrics? (usage of keyboard in sterile environment)**

Yes, there is less risk of contamination with Iris Biometrics if the sensor is mounted. The user only has to look at the sensor; they do not have to touch it to match.

**Can Iris Biometrics help with hygiene issues? (Putting finger on device without cleaning)**

Yes, there is less risk of contamination and hygiene issues with Iris Biometrics if the sensor is mounted. The user only has to look at the sensor; they do not have to touch it to match.

**Can Iris Biometrics be used in a clean room?**

Yes, Iris Biometrics can be used in a clean room. Users look at the sensor to match and sign or login. There is no contact and therefore no opportunity for contamination. There is no limitation on gowning and gloves are not an issue. The device stays in the clean room all the time and will not introduce contaminants.

**Can Iris Sensors be cleaned with chemicals? Are there any restrictions?**

Yes, Iris Biometric sensors can be cleaned with a 70% alcohol solution. Integral is presently looking into enclosures that will achieve IP68 compliance. This should be achievable with known technology as the device needs a simple enclosure with glass or clear plastic over the front to allow its camera to see and lights to illuminate the user's iris.

**Are Iris Sensors waterproof?**

No, Iris Biometric sensors are Not inherently waterproof. Integral can offer a product that is IP67 compliant and can withstand rain and cold and washdowns. It is designed for outdoor use. This product would be more expensive than a traditional indoor sensor, but would operate in a wet environment.

**Can Iris Biometrics be integrated in ISO 7 classified areas, where people wear gloves and in flammable/ small molecular areas?**

Yes, the Iris biometric can be integrated into ISO 7 areas. The unit does not require any contact to be used if mounted, so contamination is unlikely. An extra Atex compliant enclosure would be required for flammable environments. Since these enclosures can have clear glass fronts, the sensor will be able to work through the glass.

**Can Iris Biometrics be used for multiple systems? (e.g. scada, HMI logins, Pas-X, Delta v, LIMS, CW, Windows Hello…)**

Yes, the Iris Biometric is integrated with Integral's solution. Integral's solution supports numerous systems such as: Rockwell MES 8.1 and 10.2, Rockwell ViewSE for HMI Login and eSign, Camstar MESf (Portal - gray screen, and previous version - blue screen), SAP GUI 740 and 730, CDR, Compliancewire for Instructor led training and CW for rosters, Antares Vision, WunderWare InTouch HMI, Wordpress Login, Integral wearable and tablet integration tool, Integral Biometric Logbook, Integral Config Tool Login. All of these integrations can be configured to be active in the Integral Client application.

**Is Iris Biometrics more reliable than fingerprint devices?**

The Integral’s EyeLock Iris sensor has a False Accept Rate (FAR) up to 1 : 2.25 Trillion (for two eye matching). Fingerprint can range from 1 in 10,000 to 1 in 1,000,000 FAR. As for physical reliability, the product is made by an experienced electronics manufacturer VOX (AudioVox) and so should be of reliable quality. Integral has been using these products daily for the last 3 years and have not experienced any hardware malfunctions.

**Can Iris biometrics be used for access controls?**

Yes, the Iris biometric device was designed to be used in conjunction with logical and physical access control systems.

**Can Iris Biometrics replace badges?**

Yes, the Integral Iris biometric device has components available that are designed to swap into sites that have existing badge solutions without replacing the back-end components.

**Can Iris Biometrics help replace paper?**

Yes, the Integral Iris Biometric working with shop floor systems replaces paper by enabling electronic signatures. The Integral Biometric Logbook can replace HMI login paper records. The MES eSignatures enabled by our biometrics replace paper Batch records.

**What needs to be done to setup users for an Iris Biometrics system?**

To set up Iris Biometric users, the end user must work with an Enrollment Administrator and show their eyes to the sensor for about 1 - 2 minutes while using a specific enrollment application. Then the Administrator enters the end user's Name and login credentials into the enrollment application and saves their profile. Next a Biometric Administrator logs into the Integral Admin Client and brings up the end user's profile. The Administrator asks the user to look into the sensor to match. This takes a second or two and then the Administrator saves the record that has now been linked to the user's enrolled Iris matching templates and profile.

**How long does it take to setup a user to use Iris Biometrics?**

The process should take about 5 minutes per user.

**Does it require an administrator to be present to setup a user for usage of Iris Biometrics or can users set themselves up?**

End users could enroll their own Irises and add their profile, however, this would not be prudent and compliant. Users can not add their enrolled eyes to an Integral profile that contains login credentials. This requires that a Biometric Administrator logs in and saves the user record after linking their Iris profile.

**How does the Iris Biometrics authentication hardware connect to a workstation?**

The Iris sensor plugs into the workstation with a standard USB connection. The sensor can also be connected via a networked USB connection where the USB device is plugged into another compute device that has access to the same network as the intended workstation. This can be either another PC or a Raspberry Pi running the network USB client.

**Is there other hardware required beside the Iris Biometrics authentication hardware connected to the workstation?**

No, no other hardware is required to make the Iris Sensor work. However, a fingerprint sensor can be attached to the same workstation and users can use either Fingerprint or Iris to match at any part of the supported processes.

**Does the Iris senor require charging?**

No, the Iris sensor does not require charging.

**Do the Iris Biometrics devices need a continues power supply?**

The Iris Sensor only needs power when it is being used. The Iris sensor requires about 30 seconds or so to initialize, so it is not efficient to carry the sensor and plug it in each time it is needed.

**How secure is my Iris matching templates?**

The Iris sensor analyzes the user’s Iris and creates an Iris Matching template.

The Iris Matching template is encrypted on the biometric server using an encryption algorithm and then store in the biometric database. Iris Matching templates do not contain images of the Iris. Iris Matching templates cannot be used to match against other Iris Matching Templates.

**Are Iris sensors dangerous?**

The Myris device’s® camera and the two LED emitters employed in this system do not pose a potential hazard to the eyes under any foreseeable viewing conditions. Even if an individual could fixate on an emitter for many minutes, the exposure would not exceed the recommended exposure limits. Integral’s Myris Iris sensor LEDs are radiance limited and cannot produce exposure levels at the retina that even approach the levels that are known to cause retinal injury. There are also no cognizable hazards to the cornea, lens or retina of the eye from even lengthy, repeated exposures to any bystander.