RELIABLE. BIOMETRIC. SOLUTIONS.

Reference Guide - REV3

www.ievoreader.com

CONTENTS:

Before using your **ievo** system, please ensure that all required software and drivers have been correctly installed and set up by your installation provider.

Should you have any technical issues or concerns please speak to your supplier or installation provider as the first line of contact.

Welcome to Biometrics

Thank you for choosing **ievo Ltd** as your provider of biometric security solutions. Your new fingerprint reader(s) will offer a safe, reliable system to assist with your access control and /or time and attendance system. Although very simple to use, this guide will ensure you obtain the maximum benefits of your products. The guide will cover registration, usage, data protection and troubleshooting. Should you encounter any issues not covered in this reference guide please contact your provider for further support.

A LITTLE BIT ABOUT US

ievo Ltd design and manufacture a range of industry leading biometric fingerprint readers. Having spoken to professionals such as architects, facility managers, contractors, security installers and end users, our experienced team pride themselves on understanding what requirements are needed to integrate with a secure access control system. The **ievo** biometric fingerprint range has been developed with the aim of being the most technologically advanced, reliable and secure fingerprint reader on the market.

WHY BIOMETRICS?

Fingerprint biometric systems are considered to be the most reliable and trustworthy form of security due to the very nature of biometric data being unique to a sole individual. The advantage of using an **ievo** fingerprint biometric system is that common faults like; lost, stolen or copied cards/fobs; forgotten pin numbers/or access codes; hacking threats or any other form of unnecessary user interaction are all resolved. This saves time and resources while enhancing your systems.

HOW DO IEVO FINGERPRINT READERS WORK?

Simply put, by using advanced image reading sensors **ievo** readers take a highly detailed scan of your finger, from the surface and subsurface levels of the skin, to capture a highly accurate digital image. Specific data from the image is converted into a digital template used for fingerprint identification. Providing a user presents a finger that matches a stored user template, then access and/or time & attendance, will be granted and/or recorded.

The methods that **ievo** readers use to capture fingerprint data cannot be reverse engineered to replicate your actual fingerprint, nor is the data stored on the fingerprint reader head themselves, adding an additional layer of security and protection. As such we do not contravene any data protection or Human Rights laws.

USING: ievo desktop registration readers

ievo offers two variants of registration units;

The **ievo** ultimate desktop reader -

The **ievo** ultimate desktop reader is designed for use with installations using either only **ievo** *ultimate* readers, or a mixed system of both *ultimate* and **ievo** *micro* fingerprint readers.

The **ievo** micro desktop reader -

The micro desktop reader has been design specifically to work alongside installations only using **ievo** *micro* readers.

The difference is due to the size of the sensor's scanning areas on the two devices.

Once you have installed the **ievo** registration software* and are ready to register new users, make sure you follow these steps to ensure effective registration using either the **ievo ultimate** desktop reader or the **ievo** micro desktop reader.

Please ensure when using either reader that the device is on a desk and the user is standing up when registering fingerprints. This is due to the sensor's angle being optimised for an elevated approach, replicating how a user will physically use the unit for authentication. Approaching the device from a 'sitting' position during registration will provide a different reading from that of an elevated position which may cause identification errors.

For further instructions on how to enrol a user using the **ievo** registration software please see page 10.

* If using an alternative registration software package refer to documentation supplied by your provider for further assistance.

ievo ultimate desktop reader:

USING ievo, AS EASY AS...

Present finger to sensor when sensor is blue.

Once scan is complete remove finger from device.

Present finger again to confirm the registered finger.

Once scan is complete remove finger to complete the process.

Do Not Use Your Finger Tip

Do Not Bend Your Finger

Keep your finger straight and cover the whole of the sensor area

Ensure you follow the steps outlined in the registration software for optimum results.

ievo micro desktop reader:

USING ievo, AS EASY AS...

Present finger to sensor when sensor is blue.

Once scan is complete remove finger from device.

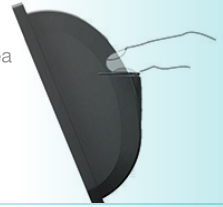
Present finger again to confrim the registrated finger.

Once scan is complete remove finger to complete the process.

Do Not Use Your Finger Tip

Do Not Bend Your Finger

Keep your finger straight and cover the whole of the sensor area



Ensure you follow the steps outlined in the registration software for optimum results.

Using ievo Standalone Software

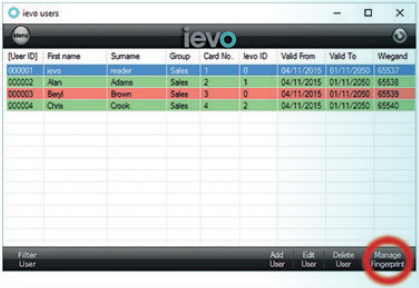
(If using alternative registration software, please refer to documentation provided by your provider)

1) Once installed launch the **ievo** Ltd registration software to open the user list screen and click ‘Add User’.

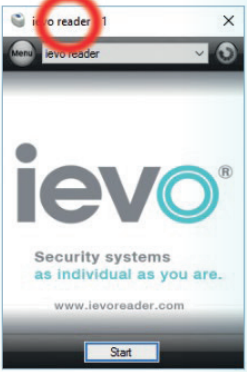
2) Enter the user’s details in the fields provided and press ‘Save’.

3) You will now see a list of registered users alongside their User ID number on the user list screen.

4) To add a fingerprint to a user, highlight the user by selecting their profile (which will turn the profile ‘blue’) and click ‘Manage Fingerprint’.
(‘Green’ profile are users with active Fingerprint Templates, ‘Red’ profiles are users without active Fingerprint templates)



5) A new ‘Registration’ screen should appear. Ensure that the correct name is displayed at the top of the window before scanning fingerprints.



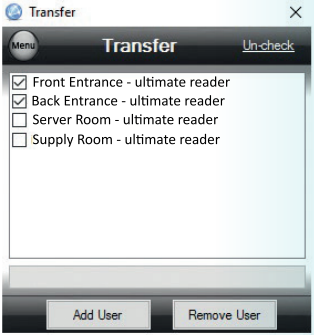
6) When ready to scan a fingerprint, press the ‘start’ button to begin. The process will prompt an initial scan of the fingerprint and then make a secondary confirmation scan (to make sure the images match). Once both images are matched you will be promted to select which readers the user will be assigned to.

6.a) The initial scan will require a finger to be placed on the registration device to register the fingerprint. Once the scan is complete remove the finger. A second scan of the same finger will then be prompted. Remove the finger once the scan is complete.

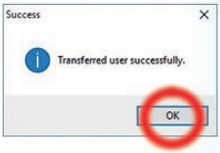
Initial scan screen

Second scan screen

6.b) Please select which ievo readers the new user will be assigned to.



6.c) Once the fingerprint has been successfully registered the 'Transferred User Successfully' message will appear and this finger can now be used for access. Please press 'OK' and close all windows.



USING THE: ievo ultimate™

Step 1:
Press the **ievo** halo to activate unit

Step 2:
Move finger away from device

Step 3:
Place finger on sensor

Step4:
Keep finger in place until scanning is complete.

Place finger in the centre of sensor....

Not to the side!

To start a scan place your finger in the centre of the scanning plate making sure that the whole area is covered, without pressing down too hard.

Using multispectral imaging the sensor will scan your finger with beams of light, gathering all the information required from between 1 - 100 individual reference points on your fingerprint.

It is vital that you keep your finger still during the scanning process to ensure there is no distortion in the image, which could lead to recognition issues. The better quality the scan, the faster the process for gaining access.

Note: If you are finding it difficult to gain access, ask a site administrator for assistance.

USING ievo, AS EASY AS...

1...

Present finger to 'halo' button to activate the reader.

2...

Move finger away from device before placing on sensor.

3...

Place finger on illuminated sensor. Do not move or remove finger during scan.

4.

Once scan complete remove finger and wait for the 'halo' button to change colour.

Green
Access granted, please processed though door.

Red
Access denied, please contact your administrator.

Do not use your finger tip

Do not bend your finger tip

Keep your finger straight

Ensure the reader has been installed in a vertical position

USING THE: ievo micro™

Step 1:
Press the **ievo** halo to activate unit

Step 2:
Move finger away from device

Step 3:
Place finger on sensor

Step4:
Keep finger in place until scanning is complete.

Place finger in the centre of sensor....

Not to the side!

To start a scan place your finger in the centre of the scanning plate making sure that the whole area is covered, without pressing down too hard.

The advance optical sensor will scan your finger with beams of light, gathering all the information required from up to a hundred individual reference points on your fingerprint.

The **ievo** *micro* scan in less that 200ms so it is essential to keep your finger still to prevent any sliding or movement that may distort the image, which could lead to recognition issues. The better quality the scan, the faster the process for gaining access.

Note: If you are finding it difficult to gain access, ask a site administrator for assistance.

USING ievo, AS EASY AS...

1...

Present finger to 'halo' button to activate the reader.

2...

Move finger away from device before placing on sensor.

3...

Place finger on illuminated sensor. Do not move or remove finger during scan.

4.

Once scan complete remove finger and wait for the 'halo' button to change colour.

Green
Access granted, please processed though door.

Red
Access denied, please contact your administrator.

Do not use your finger tip

Do not bend your finger tip

Keep your finger straight

Ensure the reader has been installed in a vertical position

User's fingerprint is not being recognised?

1. Ensure that the user has a registered profile with an active fingerprint template.

   This can be checked through your registration software.

2. Does the user have the required permissions for access?

   This can be checked and changed as required through your access control software.

3. Ensure the user is using the same finger that is registered on their user template.

   If needed, remove any previously stored fingerprint images and re-register the user's fingerprint.

4. Ensure the user is placing their finger correctly?

   Ensure the user is placing the finger correctly, face down and flat. Refer to the finger placement guides within this document.

5. Try registering a second finger as a backup.

   It is always advisable to register a second finger when possible for backup. In the instance when a user's finger is either damaged or experiencing temporary problems, having a backup image can save time during busy periods and can be looked into further when more time is available. In some cases it may be required that a user registers multiple fingers (see 'Problem Fingerprints').

6. Is the user's finger damaged?

   Any cuts, abrasions or damage on the finger could affect fingerprints as damaged skin may impair previously recorded images. Re-register the user's finger or register an alternative finger to use until the original is healed. Once healed the user may be required to re-register their fingerprint as scar tissue may be present which can alter fingerprints.

7. Has the reader been installed at the required height?

   ievo readers have instalment placement guides to allow for optimum efficiency and to be compliant with DDA regulations. Refer to the **ievo** manual for DDA compliant guidance or contact your supplier/installer if you are unsure.

8. Ensure the reader has been installed vertically.

9. Is there excessive dirt or debris on the user's finger or sensor?

   Although **ievo** readers can scan through levels of dirt and debris, having a 'clean' finger will always increase the effectiveness of the reader. Also ensure that there is no excessive dirt or debris on the reader's sensor itself before scanning.

10. Has the sensor been damaged?

    Damage to the sensor's glass can interfere when scanning a fingerprint. If there is a deep scratch or other damage present, please contact your supplier or installer.

The system is not behaving as expected.

1. Ensure that doors have not been set to 'always closed'.

   This should be controlled through your security software, please refer to software manuals for further assistance or contact your provider. **ievo** devices do not cover the actual door security permissions.

2. Check that the user is not trying to gain entry outside of allowed times.

   Check your user software that users have the required permission on their profiles.

3. Check that doors have not been bolted or locked from the inside.
4. The **ievo** reader's sensor is not responding

   Please contact your supplier or installer for technical support

If none of the above checks provide a solution to a problem you are experiencing, please contact your supplier or installer for further technical support.

TROUBLESHOOTING

My fingerprint is not being recognised?

1. Are you registered?

   Ensure that you have been registered as a user and had your fingerprint registered correctly.

2. Are you using the same finger you registered with?

   Ensure you are using the same finger that you registered with, the most common finger used is the 'index' finger.

3. Keep your finger still until the sensor finishes scanning.

   In order to get the best scan possible it is vital you keep your finger still while the sensor is scanning. Do not remove your finger until the sensor has finished its scan, the scanning process is indicated by a white light. Once complete remove your finger and wait for access.

4. Have you damaged your fingerprint?

   If you have a cut, abrasion or damage on your finger this could affect your fingerprint as damaged skin may impair a previously recorded image. Please re-register your finger, or register an alternative finger to use until the original is healed.
   Once healed you may be required to re-register your fingerprint as scar tissue may be present which can alter your fingerprint.

5. Are you placing your finger correctly?

   To ensure you are placing your finger correctly; face down and flat. Please refer to the finger placement guides within this document.

6. Is there excessive dirt or debris on your finger?

   Although **ievo** readers can scan through levels of dirt and debris, having a 'clean' finger will always increase the effectiveness of the reader.

7. Ensure that you are not pressing too heavily on the reader during a scan.

   Pressing heavily on the reader can squash your fingerprint meaning that the key reference points are spread differently from the original scan.

My fingerprint is accepted but the door does not open?

1. Check the door has not been set to 'always closed'.

   This should be controlled through your security software, please refer to software manuals for further assistance or contact your provider. **ievo** devices do not control the actual door security permissions.

2. Check that you are not trying to gain entry outside of your allowed times.

   Check with your administrator or software handler that you do not have any restricted entry times on your user profile.

3. Check the door has not been bolted or locked from the inside.

If none of these checks provide a solution to a problem you are experiencing, it could mean a faulty locking mechanism or relay. Please contact your supplier or installer for technical support.

Is my fingerprint stored on a database? If so, who has access to my information?

Fingerprint images are not stored. An **ievo** reader scans a finger and collates a range of different identifying reference points. These reference points are converted to a template and stored on an **ievo** Control Board. For more information, please read the 'Data Protection' section of this guide.

I want to know more about our biometric system and have further questions. Who can I contact?

You should contact your supplier or installer in the first instance as they will be familiar with your installation.

Alternatively you can email the **ievo** team at: **support@ievoreader.com**

or phone us Monday to Friday 9am till 5.30pm (GMT) on:

0845 643 6632 or **+44 (0)191 296 3623**

PROBLEM FINGERPRINTS

What is a 'problem fingerprint'?

While the vast majority of fingerprints can be used with **ievo** fingerprint readers there are a few occasions where some fingerprints can be tricky to capture. These instances usually occur when a finger has been heavily damaged causing permanent surface and subsurface skin abrasions. While it is uncommon, studies have shown that one out of two hundred fingerprints can be problematic when using biometric readers.

I have a problem fingerprint, can I still use biometrics?

Even though it may seem like the technology is against you, there are methods that can be attempted to combat some problem fingerprints.

What can I do to combat a problem fingerprint?

When registering a known problem finger, or if problems persist with a registered fingerprint, try registering all of the user's fingers, including the thumbs. This will help give the user a number of options when trying to gain access.

To register multiple images of the same fingerprint access the 'Manage Fingerprint' section of the **ievo** registration software. If using an alternative registration software package, please refer to your user manual or ask your software provider for assistance.

Another method is to registering multiple images of the same fingerprint from different rotational angles. Start with scanning the left side of the finger, and then registering multiple images of the finger as you roll the finger to the right (see Fig.1). This will build up a full image of the finger from different degree angles that may help with enabling the user to use the system. Keep scanning different angles until the system states a good image has been captured.

Fig.1

Start with scanning the left side of your finger, and then keep scanning different angles rotating to the right until a good scan has been captured.
If a registered finger is still not being identified, keep trying different angles.

If you continue to encounter problems with registering a fingerprint, please contact your installer for further advice.

DATA PROTECTION

What happens when my fingerprint is scanned?

When registering as a user, an **ievo** reader will scan your fingerprint and a connected **ievo** Control Board will use an extraction algorithm to identify specific features within your fingerprint called minutiae. Identified minutiae points are categorised into groups, which include line bifurcations and ridge endings amongst other data groups. During this acquisition process, the algorithm will identify the type, direction and distance between minutiae. The **ievo** Control Board then stores them in a unique proprietary template format (See Fig.1) which will be stored in a database on the control board. The original fingerprint image is not stored or recorded.

After registering a similar process described above will commence for general use. However, this time the matching algorithm will be used to compare the new minutiae data against the stored templates in the database. Once a pre-set number of minutiae points have been matched against a stored template, the user's identity can be confirmed, this confirmation will be forwarded to the access control system or 'time and attendance' system for entry access and/or data logging.

Fig.1

Image depicting what an **ievo** reader scans

Image depicting an example of key minutiae feature points taken from the fingerprint

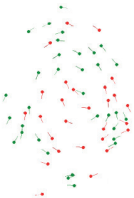


Image depicting key feature data which is extracted, transferred and stored as a template on a separate **ievo** Control Board

How is my data stored?

An advanced algorithm is used to extract specific fingerprint data captured after a scan. This data is stored on an **ievo** Control Board using a unique proprietary template format. The stored template is unique to an individual and the template is only accessed for identification purposes by the **ievo** Control Board. The data cannot be accessed for any other purpose nor can it be viewed using common software. The data CANNOT be used to re-construct the original fingerprint image.

Who has access to my fingerprint image?

No one has access to a fingerprint image as images are not stored.
Once a fingerprint has been scanned, the original image is not stored or recorded. The only stored information is the template constructed from the key features of the fingerprint and is only accessed for identification purposes by the **ievo** Control Board. The data cannot be accessed for any other purpose nor can it be viewed using common software. The algorithm is extensive in size and the template data cannot be reverse engineered to recreate an image of the original fingerprint

Can my data be accessed and used for other purposes?

No, once acquired, a fingerprint template can only be referred to by **ievo** software (via the **ievo** Control Board) for identification purposes.

Algorithms:

ievo systems use a cutting-edge Automated Fingerprint Identification System (AFIS) algorithm for data enrolment, extraction and matching processes.

FURTHER READING ON BIOMETRICS

Biometrics Explained

Biometrics refer to metrics related to human characteristics.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe an individual. Biometric identifiers are often categorised into two classifications of characteristics; physiological and behavioural.

- Physiological characteristics are related to body shape and features, for example, fingerprints, facial recognition, DNA, hand geometry, iris/retina recognition, and odour/scent.
- Behavioural characteristics are related to the pattern of behaviour of a person, including but not limited to, typing rhythm, gait, and voice.

At **ievo** Ltd we solely focus on the fingerprint physiological classifications of biometrics as a means of authentication and identity.

The very nature of biometrics being unique to the individual is of high interest and value to the security industry. Meaning that it opens up a lot of options for increased levels of security for identification purposes, which are more reliable, accurate and efficient than more traditional levels of security.

Fingerprint biometrics are unique to an individual. Built up of patterns from aggregated characteristics of ridges and minutiae points which are incredibly hard to replicate, or falsify.

Understanding the sophisticated patterns that build the structure and properties of a fingerprint is paramount to being able to successfully employ imaging technologies.

Blood vessels and other skin structures below the surface of the skin, provide an internal fingerprint pattern which in turn helps shape what we see on our fingers. These surface ridges, are formed by collagen pushing between the blood vessels in the subsurface and form what is commonly known as the 'true' fingerprint.

For further reading on Biometrics we suggest the following:

- Encyclopedia of Biometrics: I - Z., Volume 1
- http://www.biometricsdirect.com/Biometrics/biometricsterms.htm
- http://www.biometrics.gov/documents/glossary.pdf

TECHNICAL DETAILS:

ievo *ultimate* (with **ievo** Control Board) technical specifications:

CPU	ARM	
Memory	RAM 16MB FLASH 32MB	
FRR	< 0.001%	
FAR	< 0.00001%	
Identification Speed	< 0.7 sec	
Template Capacity	1:N 8,000	
Log Capacity	200,000	
Voltage	12v DC	
Current Draw	< 600mA	
Output	Wiegand	
Communication	TCP/IP IEVO/controller OEM dependent	
Operating Temp.	-20~70ºC (-4~158ºF)	
IP Rating	IP65	
Power Indicator	LED	
Certifications	CE, FCC, RoHS	
Dimensions -	**Surface:** W: 76mm (3") H: 137mm (5.4") D: 93mm (3.7")	**Flush:** W: 119mm (4.7") H: 153mm (6.02") D: 47mm recessed (1.85") Visible D: 45.5mm (1.8")

The **ievo** *ultimate* has been approved for UK Government use by the CPNI (for details contact the CPNI).

CPNI
Centre for the Protection of National Infrastructure

ievo *micro* (with **ievo** Control Board) technical specifications:

CPU	ARM
Memory	RAM 16MB FLASH 32MB
FRR	< 0.01%
FAR	< 0.00001%
Identification Speed	< 0.2 sec
Template Capacity	1:N 8,000
Log Capacity	200,000
Voltage	12v DC
Current Draw	< 400mA
Output	Wiegand
Communication	TCP/IP IEVO/controller OEM dependent
Operating Temp.	0~60°C (32~140°F)
Power Indicator	LED
Certifications	CE, FCC, RoHS, Weee, Reach
Dimensions -	W: 55mm (2.2") H: 155mm (6.1") D: 70mm (2.75")

ievo ultimate desktop reader technical specifications:

Image Resolution	500 dpi
Platen Size	18 x 28mm ellipse
Dimensions	W: 83mm L: 100mm H: 59mm
Cable length	1.8M
Template Size	1.4kB
Interfaces	USB 2.0 or above
Housing	ABS Polycarbonate mix

ievo micro desktop reader technical specifications:

Image Resolution	500 dpi
Platen Size	17.4 x 13.9mm rectangular
Dimensions	W: 65mm (55mm without stand) L: 90mm (70mm without stand) H: 180mm (155mm without stand)
Cable length	1.8M
Template Size	1.4kB
Interfaces	USB 1.1 or above
Housing	ABS Polycarbonate mix

Your supplier details are:

Need additional reference guides, user posters or further support?*

Contact ievo Ltd:

Monday to Thursday 9am till 5.30pm (GMT)
Friday 9am till 3.30pm (GMT)
Tel: **0845 643 6632** or
+44 (0)191 296 3623

*Please note that our offices are closed during national UK bank holiday periods.

ievo Ltd | Unit 5, Mercury Court | Orion Business Park | Tyne Tunnel Trading Estate | Newcastle upon Tyne | Tyne And Wear | NE29 7SN

www.ievoreader.com