



CDVI

Security to Access

ievo



ievo User Guide

Getting started with ievo biometric solutions



EN

1] CONTENTS

TITLE	PAGE
2] Welcome to Biometrics	3
3] Using ievo desktop registration units	5
4] Using the ievo ultimate reader	8
5] Using the ievo micro reader	10
6] Using ievo as a card reader	12
7] Administration guide	14
8] Troubleshooting	16
9] Problem fingerprints	18
10] Data protection	19
11] Further reading on Biometrics	21
12] Technical Specifications	22

2] WELCOME TO BIOMETRICS

Thank you for choosing CDVI and the ievo brand 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 about us

CDVI is a global manufacturer of access control solutions and with its brand ievo, is industry leading in 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 access 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.



Note

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. For further support, visit our website or alternatively contact our technical support team at:

E-mail: support.ievo@cdvi.co.uk

Tel: +44 (0) 1628 531300

3] USING ievo DESKTOP REGISTRATION UNITS

CDVI offers two variants of ievo registration units:



IEVO-UDR

The IEVO-UDR 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.



IEVO-MDR

The IEVO-MDR 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 isync 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 isync software, refer to the [isync manual](#). If you are using a different access control provider, steps might slightly change. Contact them directly for further assistance.

ievo ultimate desktop reader

			
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 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

			
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 complete remove finger to complete the process.
<p>Do Not Use Your Finger Tip</p> 		<p>Do Not Bend Your Finger</p> 	
<p>Keep you finger straight and cover the whole of the sensor area</p> 			
<p>Ensure you follow the steps outlined in the registration software for optimum results</p> 			

4] USING THE ievo ultimate READER



Step 1:

Place your finger on the sensor, which will activate via proximity detection. The sensor will glow 'blue' when activated.



Place finger in the centre of sensor...

Step 2:

Keep your finger still until the scan finishes. The 'halo' button will turn green once access has been granted.












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.

1 	2 
Place finger on sensor to activate (the sensor will illuminate). Do not move or remove finger while scan is active!	Once scan is finished, remove finger and wait for the 'halo' button to change colour.
 Green Access granted, please proceed through door.	 Red Access denied, please contact your administrator
Do Not Use Your Finger Tip  	Do Not Bend Your Finger  
Keep your finger straight  	

Ensure the reader has been installed in a vertical position.

5] USING THE ievo micro READER



Step 1:

Place your finger on the sensor, which will activate via proximity detection. The sensor will glow 'blue' when activated.



Place finger in the centre of sensor...

Step 2:

Keep your finger still until the scan finishes. The 'halo' button will turn green once access has been granted.






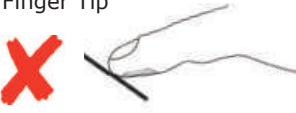

Not to the side!

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 than 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.

<p>1.</p> 	<p>2.</p> 
<p>Place finger on sensor to activate (the sensor will illuminate). Do not move or remove finger while scan is active!</p>	<p>Once scan is finished, remove finger and wait for the 'halo' button to change colour.</p>
 <p>Green Access granted, please proceed through door.</p>	 <p>Red Access denied, please contact your administrator</p>
<p>Do Not Use Your Finger Tip</p> 	<p>Do Not Bend Your Finger</p> 
<p>Keep your finger straight</p> 	

Ensure the reader has been installed in a vertical position.

6] USING ievo AS A CARD READER

Card Reader Functions

ievo fingerprint readers can be upgraded with a card reader module to allow for combined use of both biometrics data and security cards. Using the HID iCLASS SE™ reader module you will be able to utilise existing card reader systems through ievo reader units. To check that your cards are compatible with the module please contact us.

There are 3 functions available :

Pass through

Usually used in areas where there is a transition period moving from card readers to biometrics, or for visitor access only. A user will just need to present their card to the reader's 'halo' to be verified.

1:1 Template on card

Used in environments whereby a user's fingerprint template data is stored on a security card. Users will present their card to the reader's 'halo' which will tell the reader to expect a finger to be presented. The reader will scan the user's finger and compare this with the biometric template stored on the card for verification.

Multimodal

Offering two options; to either use both the card reader and the fingerprint reader as a primary and secondary verification unit (i.e. two levels of verification are needed for identification, set-up via an access control system), or to use both methods of identification in an 'either or' situation. Meaning if a user forgets, loses or damages their security card, they can use the biometric function, or if they are wearing heavy gloves, or have damaged their registered finger, the card reader function can be utilised.



Our readers use highly accurate sensors and when combined with the card reader module the opportunities to compromise the identification phase reduces to virtually zero.

However you are using the card reading functions on your ievo reader, the process is the same:



7] ADMINISTRATION GUIDE

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. 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.

8. 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 can be checked through your access control software. ievo devices do not control door access.

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

Check within your access control software that users have the required permissions on their profiles.

3. The ievo reader's sensor is not responding.

Please contact your supplier or installer for technical support.

4. The ievo reader's 'halo' button is flashing white.

This indicates that the ievo reader is re-establishing a connection with the ievo interface board and should function as normal once the halo has returned to the normal blue LED light.



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.

8] 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 to not press 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 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.

2. 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 interface 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.



For further support, visit our website or alternatively contact your local Technical Support team:

E-mail: support.ievo@cdvi.co.uk

Tel: +44 (0) 1628 531300

9] PROBLEM FINGERPRINTS

What is a 'problem fingerprint'?

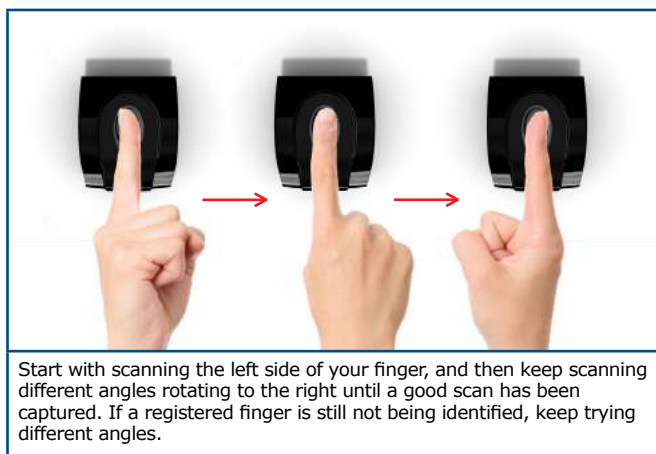
While the vast majority of fingerprints can be used with ievo fingerprint readers there are a few occasions where some fingerprints can be tricky to capture. These instances usually occur when a finger has been heavily damaged causing permanent surface and subsurface skin abrasions. While it is uncommon, 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.






You can enrol multiple images of the same finger from different angles, such as lying your finger on both its sides and mid section.

10] 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 interface 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 interface board then stores them in a unique proprietary template format (see table below) which will be stored in a database on the interface 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.

		
Image depicting what an ievo reader scan	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 interface 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 interface 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 interface 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 Interface 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 interface board) for identification purposes.

11] 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 CDVI, we solely focus on the fingerprint and facial 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.

12] TECHNICAL SPECIFICATIONS

ievo ultimate

Description	Data
CPU	ARM
Connection	Shielded (S-FTP) Cat5e/6 cable
Voltage	12V
Current Draw	600mA
Communication	RS-422 (1Mbit/s)
Controller	ievo interface board (IEVO-MB10K, IEVO-MB50K)
Operating Temperature	-20~70°C
Power Indicator	LED
IP Rating	IP65
Certifications	CE, UKCA, FCC, NPSA
Dimensions	Surface Mount: 128mm (H) x 93mm (W) x 93mm (D)
	Flush Mount: 153mm (H) x 119mm (W) x 47mm (D/ recessed) or 45.5mm (D/visible)

ievo micro

Description	Data
CPU	ARM
Connection	Shielded (S-FTP) Cat5e/6 cable
Voltage	12V
Current Draw	400mA
Communication	RS-422 (1Mbit/s)
Controller	ievo interface board (IEVO-MB10K, IEVO-MB50K)
Operating Temperature	0~60°C
Power Indicator	LED
Certifications	CE, UKCA, FCC
Dimensions	Surface Mount: 155mm (H) x 55mm (W) x 70mm (D)
	Flush Mount: 230mm (H) x 80mm (W) x 33mm (D)

ievo Interface Board

Description	Data
CPU	ARM @ 454MHz or 528MHz
Memory	RAM 256MB Flash 256MB
Identification speed	From 400ms (depending on database size)
Template Capacity	10,000 or 50,000, 1:1 or 1:N
FRR	< 0.01%
FAR	< 0.00001%
Log capacity	200,000 rolling
Communication with Network	TCP/IP (100Mbit/s full duplex)
Communication with Reader Unit(s)	RS-422 (1Mbit/s)
Connection to Reader Unit(s)	Shielded (S-FTP) Cat5e/6 cable
Current Draw	400mA - 1.2A (head dependant)
Output	Wiegand 26-bit, 34-bit, 44-bit Clock and data TCP + more
Power Indicator	LED
Power Options	AC/DC 12-24V / PoE IEEE 802.at
Certifications	CE, UKCA, FCC
Dimensions	128mm (H) x 93mm (W) x 27mm (D)

ievo Registration Units

	ultimate	micro
Sensor type	Multispectral Imaging (MSI)	Enhanced Optical
Image Resolution	500dpi	500dpi
Cable length	2m	2m
Interfaces	USB 2.0	USB 1.1 or 2.0
Housing	PC/ABS mix	PC/ABS mix
Dimensions	66mm (H) x 69mm (W) x 99mm (D)	171mm (H) x 64mm (W) x 121mm (D)

CDVI Group

FRANCE (Headquarters)

Phone: +33 (0) 1 48 91 01 02

.....

CDVI FRANCE + EXPORT

+33 (0) 1 48 91 01 02

www.cdvi.fr

CDVI AMERICAS

+1 866 610 0102

www.cdvi.ca

CDVI BENELUX

+32 (0) 56 73 93 00

www.cdviBenelux.com

CDVI GERMANY

+49 (0) 251 798477 0

www.cdvi.de

CDVI SUISSE

+41 (0) 21 882 18 41

www.cdvi.ch

CDVI IBÉRICA

+34 (0) 935 390 966

www.cdviiberica.com

CDVI ITALIA

+39 (0) 321 90 573

www.cdvi.it

CDVI MAROC

+212 (0) 5 22 48 09 40

www.cdvi.ma

CDVI NORDICS

+46 (0) 31 760 19 30

www.cdvi.se

CDVI UK

+44 (0) 1628 531300

www.cdvi.co.uk

CDVI POLSKA

+48 (0) 12 659 23 44

www.cdvi.com.pl

All the information contained within this document (pictures, drawings, features, specifications and dimensions) could be perceptibly different and can be changed without prior notice. - May 2024