USER MANUAL

iPB 7

BUSINESS SOLUTION

LOBAL NETWORK

iPulse
systems

WARNING & NOTICE

The information provided in this document is the sole property and copyright of iPulse Systems, and all rights are reserved *in toto* with respect to this copyright.

Whilst this information is provided freely to users of the iPulse product range, the information is provided for a specific purpose and may not be copied, redistributed, reproduced or shared in whole or in part, without the express written permission of iPulse Systems.

Furthermore, the information contained in this document may not be shared with other users for any other purpose than the requirement to install or use the relevant iPulse product.

Where other company names or products are referenced in this manual, iPulse Systems acknowledges that these are trademarks of their respective owners and has indicated as such with the symbol ™ or ®.

REVISION HISTORY

REVISION HISTORY			
Rev	Description of Change	Author	Effective Date
01	Initial Release	GM Chalmers	September 2017
02	Updated Release – Full Edit and Review	GM Chalmers	March 2018
03	Fixed Minor Errors/ Changed Cover Design	GM Chalmers	April 2018
04	Updated Release – Additional Features & Troubleshooting	GM Chalmers	July 2018
05	Updated Release – Additional Features & Errata	GM Chalmers	September 2018
06	Updated Release – Additional Features & Errata	GM Chalmers	February 2021

REFERENCE DOCUMENTS

REFERENCE DOCUMENTS	
Document Number/Location	Document Title
Download Link: Click Here	**IQSuite.Cloud** USER GUIDE
Download Link: Click Here	iPulse Systems – User Data Privacy Policy
Download Link: Click Here	iPulse Systems –Product Terms of Use

TABLE OF CONTENTS

Table of Contents

TABLE OF FIGURES

SECTION 1
INTRODUCTION & OVERVIEW

1.1 Introduction

Thank you for choosing to purchase an iPulse Systems biometric reader. We are aware that there are many options to choose from and are grateful that you have elected to choose our products out of the many competitive options available to you.

The iPulse iPBx range of biometric devices are made with care and pride, and with proper installation and care, should provide many years of uninterrupted service. The following guide is intended to assist you to properly understand the best methods for installing and maintaining your product.

1.2 A quick overview of the iPBx biometric device range

The iPulse iPBx biometric device range use a simple combination of numbers and names to help users clearly understand the type of device. In general, all products are named as follows:

iPB**x** <**Name**> <**Description**>

- The **x** above is a number, between 1 and 9, which represents model of the biometric reader.
- The <**Name**> represents the type, which explains the features, most of which are common across models.
- The <**Description**> normally reflects the card supported by that specific model and is normally only included with Identity models.

For example, an iPB7 Identity SE/Prox, means that the reader is an iPB7 model, of the type Identity (a reader type that has a built-in card reader, with the description SE/Prox meaning that this specific card reader supports the HID SE (multiclass) card reader, as well as the multiclass Prox card reader.

Typical product types are the following:

Access: Normally a “dumb” device, the Access does not have its own controller built in. Designed to work specifically with the IntelliControllers™, Access devices do on-device fingerprint matching, but use the “brain” of the IntelliController™ for all other processing. Typically, these devices are used in environments with smaller user bases, and where cost is a key driver.

Enterprise: The Enterprise range offers the full built-in controller that the iPBx range of biometric devices are famous for. Offering full redundancy, and with complete operation in both online and offline modes, the Enterprise range of readers are the core of the iPulse range.

Identity: The Identity range offers the same features as the Enterprise, but with built-in card readers for sites who wish to use a combination of fingerprint and card, or in some cases, offer both options separately. Depending on the card types offered, Identity models can work as fingerprint only, card only, card to identify and fingerprint to verify or even fingerprint on card for local matching only.

1.3 Understanding the IntelliDevice™ and IntelliLink™ Architecture

The iPulse iPBx biometric device range use the unique IntelliLink™ to make connections simple, yet extremely powerful. The IntelliLink™ is a patented way for iPulse devices to share power, network communications and iPulse-specific communications with each other, and connects a family of devices known as IntelliDevices™, the most common of which is the IntelliRelay™.

All iPBx biometric devices ship with an IntelliRelay™ in the box. This extremely powerful device acts as the readers connection to the outside world, providing network, power, and communications, and including a highly secure and extremely powerful relay board that can trigger external devices such as a mag lock, receive feedback or status signals from external devices, and, accept a push button input.

Because the IntelliRelay™ is "Intelligent", it can monitor these inputs, and report back to the reader, turning even a "dumb" push button device into a monitored and recorded input. Furthermore, the IntelliRelay™ can monitor the biometric device itself, and should it lose connection for any reason, perform an auto-reset of the reader, thus ensuring maximum uptime.

Using commonly available RJ45 connectors, the iPBx range of readers connect directly to the IntelliRelay™ via standard Category 5e (***1**), commonly known as Cat 5 cable.

***1** For a better understanding of Cat 5 cabling, visit Wikipedia:
https://en.wikipedia.org/wiki/Category_5_cable

1.4 SecuGen Sensor & Capture/ Matching Algorithm

The iPulse iPBx range of biometric devices come standard with the SecuGen range of FBI-certified, patented SEIR-based fingerprint sensors and uses the Secugen MINEX-tested/ NIST-compliant algorithm for capture and matching.

SecuGen Corporation is one of the world's leading provider of advanced, optical fingerprint recognition technology, products, tools, and platforms and has been serving the global biometrics industry since 1998.

The iPBx readers use the SecuGen Corporation MINEX Compliant Extractor and Matcher, and the following information shows the SDK Code and CBEFF PID relating to these specific products. MINEX is a project of NIST's Information Technology Laboratory's Information Access Division, and NIST is an agency of the U.S. Commerce Department's Technology Administration, and more information pertaining to these values, and how they are calculated, is available from their website.

MINEX Compliant Feature Extractor

Organization Name	SDK Code	Extractor CBEFF PID (hex)	Software Identification
SecuGen Corporation	1G	000A0035	SecuGen ANSI INCITS 378 Template Generator v3.5

MINEX Compliant Matcher

Organization Name	SDK Code	Extractor CBEFF PID (hex)	Software Identification
SecuGen Corporation	1G	000A8035	SecuGen ANSI INCITS 378 Template Matcher v3.5

1.5 Products Covered in this Manual

This manual covers the entire range of the iPB7 biometric devices, including the following models:

iPB7 Model #	Fingerprints	Contactless Smartcard Reader			IP65 Rated *2
		SEOS®, iClass® *1	Prox®	MIFARE®, DESFire®	
iPB7 Enterprise	20,000 templates	----	----	----	✓
iPB7 Identity MiFare	20,000 templates	----	----	✓	✓
iPB7 Identity Prox	20,000 templates	----	✓	----	✓
iPB7 Identity SE	20,000 templates	✓	----	✓	✓
iPB7 Identity SE/Prox	20,000 templates	✓	✓	✓	✓

Figure 1 - Understanding iPB7 Models

1 *HID SE Multiclass® readers provide support for the following card types: SEOS®, iClass®, MIFARE®, DESFire® and where specifically indicated, Prox® as well.*

2 IP65 rating is an international standard that measures the dust and water resistance of a device. Properly installed with the optional mounting plate and rain cover, the iPB7 range is fully IP65-compliant. For complete & detailed installation instructions, see SECTION 6 INSTALLATION GUIDELINES in this manual. To understand IP ratings, see Appendix A of this manual. IP compliance is as much a factor of installation as manufacture, and the installer plays a critical role in ensuring that the device meets these requirements.

3 IP65 rating is an international standard that measures the dust and water resistance of a device. Properly installed with the optional mounting plate and rain cover, the iPB7 range is fully IP65-compliant. For complete & detailed installation instructions, see SECTION 6 INSTALLATION GUIDELINES in this manual. To understand IP ratings, see Appendix A of this manual. IP compliance is as much a factor of installation as manufacture, and the installer plays a critical role in ensuring that the device meets these requirements.

SECTION 2
SAFETY INSTRUCTIONS

The iPBx range of biometric readers have been designed foremost with safety and ease of installation in mind. All our products are DC (Direct Current), 12V (low voltage) devices, and as such, do not specifically require the availability of a certified wireman when being installed.

Using commonly available RJ45 connectors, the iPBx range of readers connect directly to the IntelliRelay™ using standard Category 5e network cable (***1**), commonly known as Cat 5 cable. This cable provides the reader with power, network communications, and the unique iPBx IntelliLink™ connection, which will be explained further in later chapters.

***1** For a better understanding of Cat 5 cabling, visit Wikipedia:
https://en.wikipedia.org/wiki/Category_5_cable

Whilst the iPBx readers use standard or conventional cabling, they do **NOT USE A STANDARD WIRING** convention. This is for multiple reasons, including the following:

Security: A big concern for any company is physical access to their networks. iPBX biometric devices often sit outside a building, as they are required to grant access. To ensure that the device cannot simply be removed from the wall, and used by any other device for internet access, iPulse mixes up the cabling to ensure that only iPBX devices can access the network through the IntelliRelay.

Distance Standard Cat 5 cables support a distance of up to 100m. To make sure that all of our signals, including power (***1**), can run this distance, iPulse uses a specific cable pattern to reduce interference, and boost signals. Therefore, in distances over 5m, only the iPulse cabling method will work.

> ***1** *All iPBx devices require a standard 13,8v input, and supplying voltage that is higher than this can cause significant damage to the device. Having said this, voltage drops over distance, and as such, when the distance between the iPBx device and the IntelliRelay™ reaches greater than 40m, it is advisable to seek expert advice on how to inject higher voltages at the opposite end to allow for the drop over distance that the readers will experience. No greater than 17v should EVER be inputted to an IntelliRelay™ however, to avoid damaging the unit.*

The following diagram – which is very similar to the TIA/EIA 568B standard, should be used for all cables linking an iPBx device to an IntelliRelay™. The only key difference – and the easiest way to remember this diagram, is that all colours should be paired together, unlike the TIA/EIA 568B standard, where the middle 4 cables are mixed up.

In general, ANY wiring diagram where all pairs are together, ie, Orange and White, Orange, then Green & White, Green, then Blue & White, Blue, and finally Brown & White, then Brown, is acceptable.

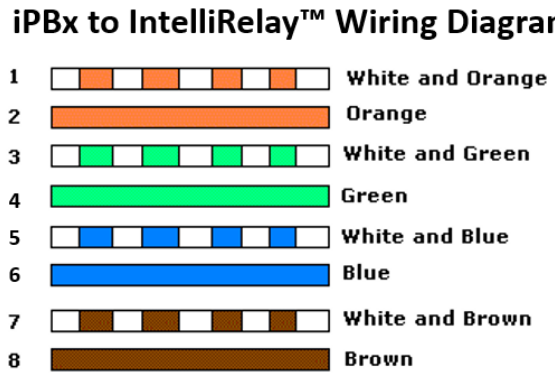


Figure 2 – iPBx to IntelliRelay Wiring Diagram

There is no reason that anyone who is certified to work on standard networking cables cannot work on the wiring between the iPBx devices, and the IntelliRelay™. Many network cables which use the PoE standards contain much higher voltages than the IntelliRelay™ puts out.

Having said this, the IntelliRelay™ itself connects to a power supply directly, and this power supply is normally connected to the AC (Alternating Current) mains electrical supply. Although this power supply is not a direct part of the iPBx installation, it is highly recommended that only a certified wireman connects the power supply to the mains power supply, and that even the connection of such a supply to the IntelliRelay™ via the 12V output should be performed by the same person if possible.

It is highly recommended that a good quality (at least class II) power supply be used, which supplies a minimum of 1A output at 12V DC. All power supplies should conform to the Safety Electrical Low Voltage standards and should always be earthed where possible.

The iPBx range of biometric products were tested using power supplies that meet the UL60950-1, TUV EN60950-1, CCC GB4943(RS-50 only) safety standards, and when used in conjunction with this type of power supply, are known to conform to the Safety Electrical Low Voltage standards.

For wires connecting from the power supply to the IntelliRelay™, it is recommended that AWG20 (***2**) cable be used, and that this distance should not exceed 10 meters from the power supply to the biometric reader. Where possible, and for maximum reliability, a length of 5 meters is recommended, and preferred.

***2** For a better understanding of the AWG wiring standards, visit Wikipedia:
https://en.wikipedia.org/wiki/American_wire_gauge

Prior to connecting the iPBx reader to the IntelliRelay™, a voltage measure of the power input block should be taken. This should measure between 12V (minimum) and 13,8V (maximum). Lower voltages could provide insufficient power for the device to run correctly, and higher voltages could damage the IntelliRelay™ which has surge protection circuitry, and is thus designed to switch off, or even blow, if too much voltage is supplied, to protect the biometric reader.

When connecting your iPB7 to a power supply, it is important to know how much power the device will draw at peak, and what the average consumption is. This is very important especially when connecting the device via PoE.

	Amps	Watts
Overall Average	309mA	4.09W
Minimum Average	295mA	3.91W
Maximum Average	323mA	4.28W

iPulse recommends that a **minimum power supply of 500mA or 8W** is supplied when connecting the device to a power source. Having said this, it is critical to understand that if connecting a maglock or striker lock to the same power source, that the current draw of these devices needs to be considered.

In the case where both the iPB7 and a locking mechanism are connected, it is recommended that a **minimum power supply of 1,5A or 17W** is supplied. This is subject to the power draw of the locking mechanism, and care should be taken to ensure that enough power is supplied in cases where these devices are using more than average.

If you are uncertain, consult an electrical contractor, especially in cases where you are using PoE to power these devices, as whilst they may appear to work during installation, continued use of an under specified power supply could result in problems over time.

IMPORTANT SAFETY WARNING

As with all electronic devices, the iPBx biometric device range can experience electronic malfunctions. Whilst all the iPulse products are designed with safety in mind, and thus have multiple methods to ensure that such failures happen in a safe and controlled manner, it is always wise to assume that anything abnormal you can see, smell or hear are not safe, and thus the device should be disconnected from the power source immediately.

Any strong metallic odour, or sounds of popping, crackling or hissing, are normally clear indicators that something is not right with the device, and any visible signs of smoke should also be taken very seriously.

Always put safety first, and if you experience any of the above, contact your product channel for assistance and guidance.

SECTION 3
REGULATORY & ENVIRONMENTAL

3.1 Regulatory Overview

As this is an electronic device, it is governed by different regulations and standards around the world. To comply with these standards, iPulse performs rigorous compliance & safety tests through registered test centres across the globe and uses these results to apply for certification from different authorities and bodies.

As many of these standards are self-regulated, iPulse stores copies of all test results, and related documentation, in physical files, which are kept at various addresses depending on the requirements of the specific standard.

At a minimum, iPulse keeps copies of all documentation at its South African headquarters, which are based at the following address:

iPulse Systems
Unit 15A Skyview Retail Park
Stridjompark, Randburg
South Africa

Please feel free to contact us should you have any specific requirement to view this information, which will be disclosed to anyone in compliance with the regulations associated with making this information available for specific purposes.

3.2 FCC Regulations – United States of America

The Federal Code of Regulation (CFR) FCC Part 15 is a common testing standard for most electronic equipment. FCC Part 15 covers the regulations under which an intentional, unintentional, or incidental radiator can be operated without an individual license. FCC Part 15 covers as well the technical specifications, administrative requirements and other conditions relating to the marketing of FCC Part 15 devices. Depending on the type of the equipment, verification, declaration of conformity, or certification is the process for FCC Part 15 compliance.

More information about FCC certification can be found on Wikipedia at the following web address: https://en.wikipedia.org/wiki/FCC_Declaration_of_Conformity

The iPB7 range of biometric devices has been extensively tested and found to be compliant with **Part 15 of the FCC Rules**, under which it is defined as a **Class A Digital Device**.

A Digital Device is defined as an unintentional radiator (device or system) that generates and uses timing signals or pulses at a rate in excess of 9,000 pulses (cycles) per second and uses digital techniques; inclusive of telephone equipment that uses digital techniques or any device or system that generates and uses radio frequency energy for the purpose of performing data processing functions such as electronics computations, operations, transformations, recording, filing, sorting, storage, retrieval, or transfer.

Furthermore, the iPB7 range of biometric devices are defined as Class A Digital Devices, which means that they are marketed for use in a commercial, industrial, or business environment, but not in a residential environment.

It is important to understand that any unauthorized changes made to the device could void the end users authority granted under these rules to use the equipment, and therefore, these devices should only be used in the manner described in this user manual or in other official iPulse documentation pertaining to product usage.

3.3 CE Regulations – European Union

The CE mark is a conformity marking for electronic products sold with the European Economic Area (EEA) since 1985. It is a world-wide recognized symbol, which is like the FCC defined in 3.2 above. To be CE compliant, the iPBx range of devices is required to conform to a number of directives, which include the following:

- EMC Directive 2014/30/EU
- Low Voltage Directive 2014/35/EU
- RoHS Directive 2011/65/EU

More information about CE certification can be found on Wikipedia at the following web address: https://en.wikipedia.org/wiki/CE_marking

The iPB7 range of biometric devices has been extensively tested and found to be compliant (or conformant) with the above-mentioned directives.

3.4 SABS Regulations – South Africa

SABS, or the South African Bureau of Standards, provide certification to industry in South Africa and beyond since 1980. The SABS brand is synonymous with quality, reliability and dependability and is found across all manner of products, including electronic products such as the iPBx range of biometric readers.

More information about SABS certification can be found on the SABS website at the following address: https://www.sabs.co.za/

The iPB7 range of biometric devices has been extensively tested and found to be compliant with the SABS standards applicable to electronic devices.

3.5 Waste Disposal

iPulse Systems is a strong supporter of managing electronic waste, and we comply to the regulations, both proposed and legislated, that relate to Electronic Waste Recycling in the USA, South Africa and across Africa. For more information pertaining to electronic waste disposal, please visit the following link, which contains many helpful references and an abundance of information:

http://www.calrecycle.ca.gov/electronics/reginfo/default.htm

In general, no electronic devices should be disposed of with your regular garbage, and there are many companies available who assist with this disposal if necessary. Should you be uncertain of where to dispose of these items, you may return them directly to iPulse Systems, at the following address, and we will dispose of them on your behalf in the correct manner:

iPulse Systems
Unit 15A Skyview Retail Park
Stridjompark, Randburg
South Africa

SECTION 4
UNPACKING THE BOX

Thank you for purchasing an iPulse iPB7 Biometric device. Your iPB7 should be packaged neatly into a sturdy and securely built box, clearly branded with the iPulse brand, and your device name.

When opening the box, you should find your biometric reader and IntelliRelay™ securely packaged in a high-density foam casing, which has been carefully selected to provide your product with maximum protection during shipping. The front cover of the reader should be nestling on top of the actual reader. *See Figure 3 - Box Interior*

Figure 3 - Box Interior

On the side of the box there will be a product serial number as well as a sticker to show the specific model of the device you have purchased (*see Figure 4 - Serial & Model*). This is important information & the serial number on the box should correspond with the serial number on the unit inside the box.

If for any reason this is NOT the case, please report this immediately to the supplier who provided you with your reader.

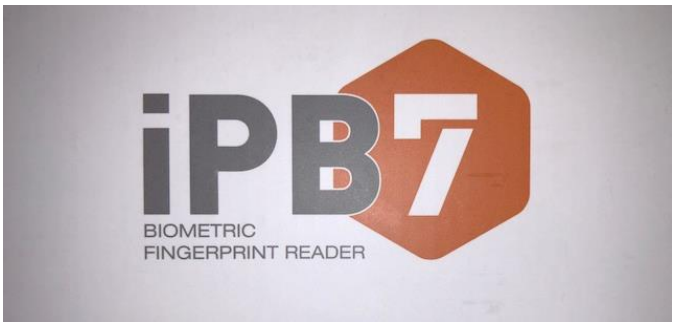


Figure 4 - Serial & Model

An instruction and care leaflet should also be in the box. This should be read carefully as it has a lot of valuable information about caring for your reader, and where to find software and support should you require any.

Unpacking the box should provide you with an IntelliRelay™ which is your reader's connection to the outside world. There is a wiring diagram provided for convenience on the top of the IntelliRelay™ casing. You should also find an iPB7 Biometric device, which consists of two parts: the fully assembled and sealed iPB7 biometric unit, and a front cover that can be put on after installation.

At the time of packaging, the iPB7 biometric unit should be inside a clear plastic bag, whilst the front cover should be loosely lying on top of it, and not actually clipped in or joined in any way. (*see* Figure 5 – iPB7 device, front casing & IntelliRelay).

Figure 5 – iPB7 device, front casing & IntelliRelay

Finally, and if you look at the rear casing of the iPB7 biometric device, you should also see a sticker that has some important information on it. Some, or perhaps all, of this information will be needed during the configuration of the iPB7 reader, depending on which software solution you are using it with, and the specific requirements of your network.

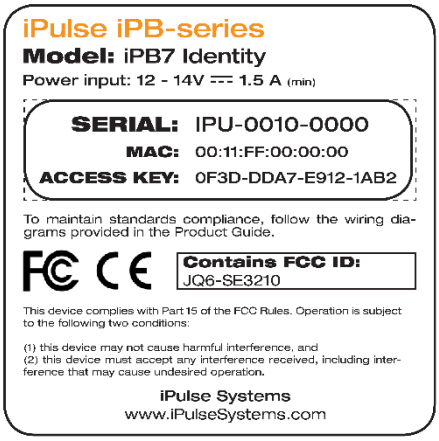


Figure 6 - iPB7 Information Sticker

It is therefore extremely important that you make a note of all this information BEFORE installing the unit and save it in a safe and secure place for future use, or when requested by the network or software engineer who is configuring the iPB7 biometric device.

The information that you need to save is as follows:

Serial: The serial number of the reader, normally in the format IPU-0000-0000, is a unique identifier issued and created by iPulse for every device they sell. This serial number is used to determine the warranty period of the device, and to track its movement history from the time it was manufactured until its eventual removal from service. This number will be required in all communications with iPulse or any of its distributors or resellers when requesting support, service, or information. It is also used with the **IQSuite Cloud 5.x** solution when adding a device to the database.

MAC: The MAC address, as defined by Wikipedia, is a media access control **address** (**MAC address**) of a computer (sic), and is the unique identifier assigned to network interfaces for

communications at the data link layer of a network segment. **MAC addresses** are used as a network **address** for most IEEE 802 network technologies, including Ethernet and Wi-Fi.

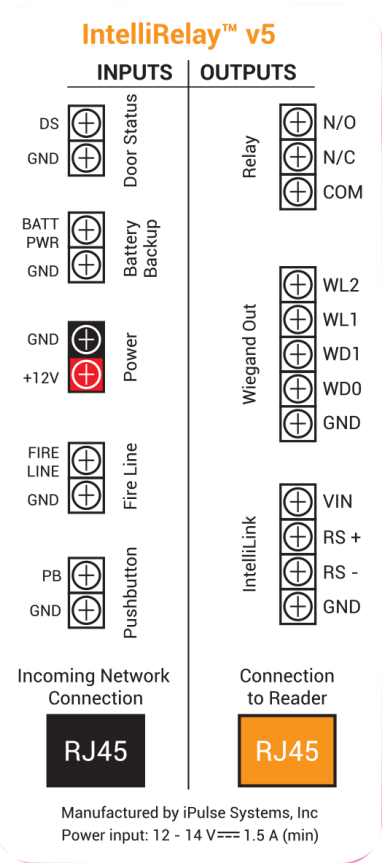
As the iPBx biometric device is in effect a computer, running the Linux operating system, it too has a unique MAC address, taken from the iPulse Systems pool of MAC addresses. This address will be needed when configuring the device on multi-layer switches, as well as when using the iPBx with certain software, such as **IQSuite Cloud 5.x**.

It is useful to know that all iPulse MAC addresses begin with **00:11:2D**.

Access Key: The Access Key is a unique security key allocated to your device and is specifically required when connecting your iPBx to **IQSuite Cloud 5.x**. This key, when combined with the serial number of the iPBx, gives significant control to a user, and the key should thus be carefully and safely stored for future reference.

SECTION 5
IntelliRelay™ CONNECTION

The IntelliRelay™ v5 acts as the main connection point between the iPBx biometric device and the outside world.



The section on the left of the IntelliRelay™ is reserved for Inputs, whilst the section on the right provides output. The IntelliRelay™ is designed to function on 12 – 14 V DC and should be connected to a Power Supply providing at least 1.5A, especially if the device is being used to trigger a mag lock or electronic door striker.

Inputs

- **Door Status** – connection terminals for the door status monitor, used to determine the state of a door (or another connected device)
- **Battery Backup** – this allows the relay to determine if it is running off a battery backup unit and to send notifications if configured to do so.
- **Power –** connection terminals for the power supply, providing power to both the IntelliRelay and the connected iPB4.
  Note that whilst this unit has significant protection against electrical surges, polarity is still important. Incorrect wiring could severely damage the IntelliRelay™.
- **Fire Line** – connection terminals for a fire system. This needs to be turned on with a switch INSIDE the IntelliRelay™ to operate and requires the presence of a 5v signal to keep operating.
- **Pushbutton** – connection terminals for an exit button or touchless exit sensor.
- **Network Input** – incoming network connection is plugged in here and passed through to the iPB4 to simplify installation and avoid exposing a network point to the outside world.

Outputs

- **Relay –** connection terminals for the on-board relay. Provides **Normally Open (N/O), Normally Closed (N/C)** and **Common (COM)** terminals.
- **Wiegand Out –** connection terminals for Wiegand output, allowing communication with Wiegand-compatible controllers and similar devices. Also allows for feedback from a controller if wired correctly and configured for this response in **IQSuite.cloud**.
- **IntelliLink –** connection terminals for the IntelliLink connection that allows several IntelliRelay™ to be daisy-chained to support additional functionality through use of a single device.
- **Reader Connection –** RJ45-type connector used to provide power and communications to a connected iPB7.

Wiring Diagram – Fail Closed

This is the most common wiring diagram and is used when a door needs to be configured in such a way that if the power is cut, the door remains locked.

High security doors, such as entry/exit doors to buildings, should always be wired with this configuration, but it is important to note that there should always be an override switch, especially on the inside, in case of fire.

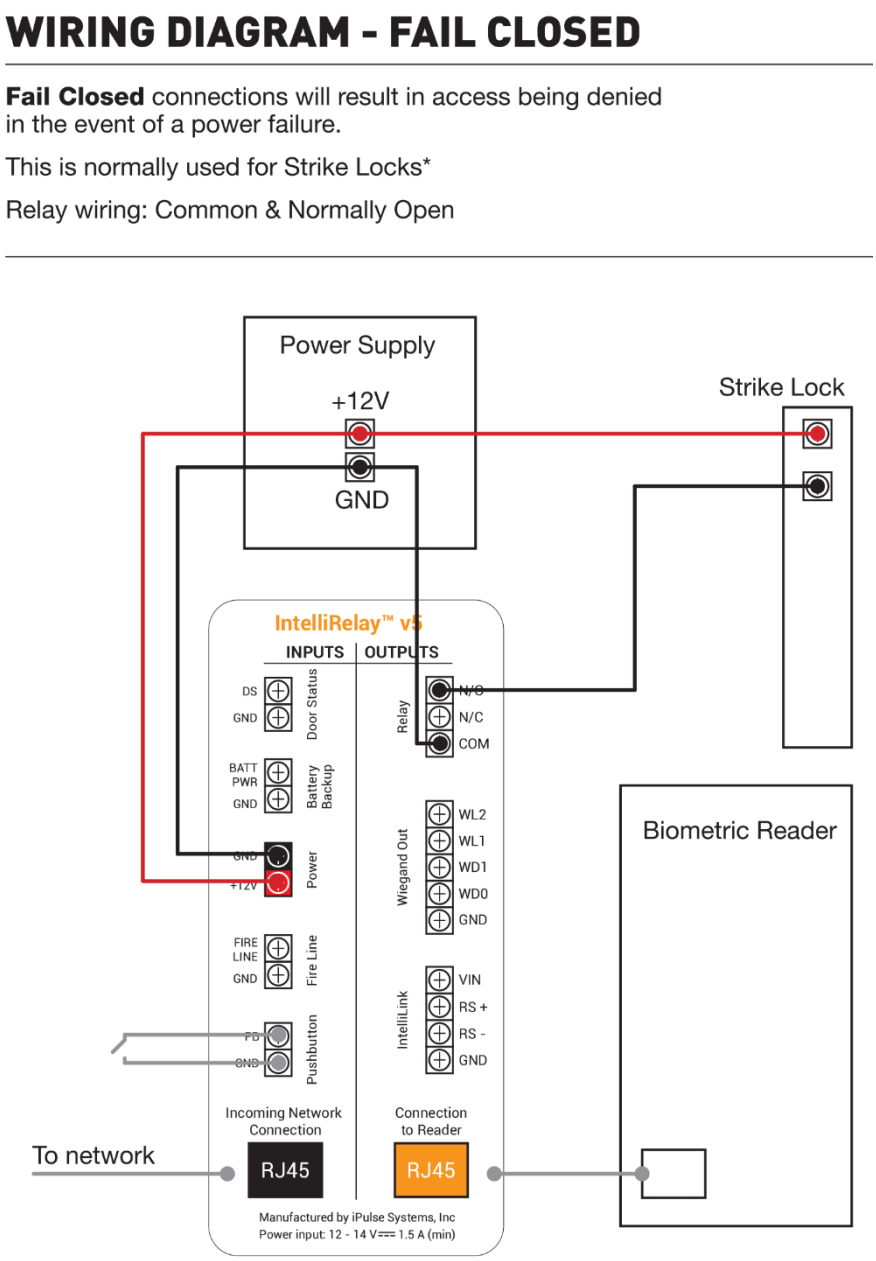


Figure 7 - Wiring Diagram - Fail Closed

Wiring Diagram – Fail Open

This is a less common wiring diagram, and it is normally used when a door needs to be configured in such a way that if the power is cut, the door remains open. This normally applies to non-critical internal doors.

WIRING DIAGRAM - FAIL OPEN

Fail Open connections will result in access being granted in the event of a power failure.

This is normally used for Mag Locks*

Relay wiring: Common & Normally Closed

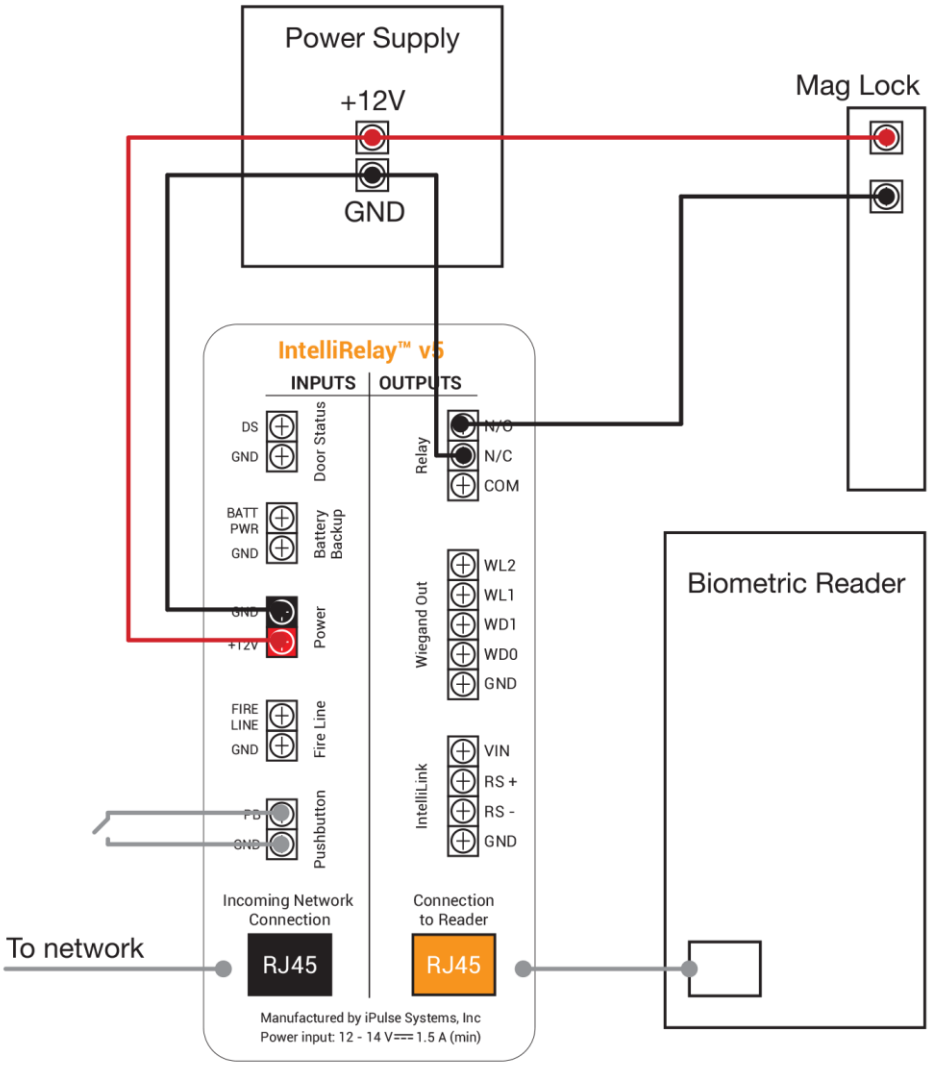


Figure 8 - Wiring Diagram - Fail Open

IMPORTANT SAFETY WARNING

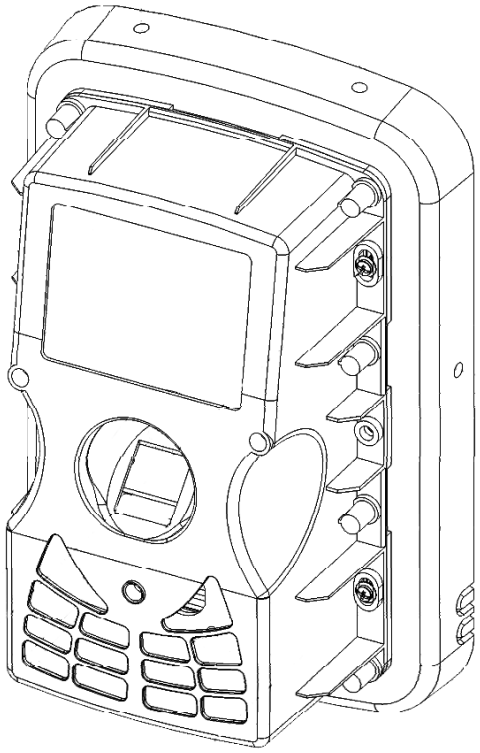
Cables are loose and exposed, and so could be touched by mistake. Therefore, the IntelliRelay™ needs to either be installed in the ceiling, where it is meant to be, or if placed in a spot where it can be reached, it should be mounted into an electrical housing for safety reasons.

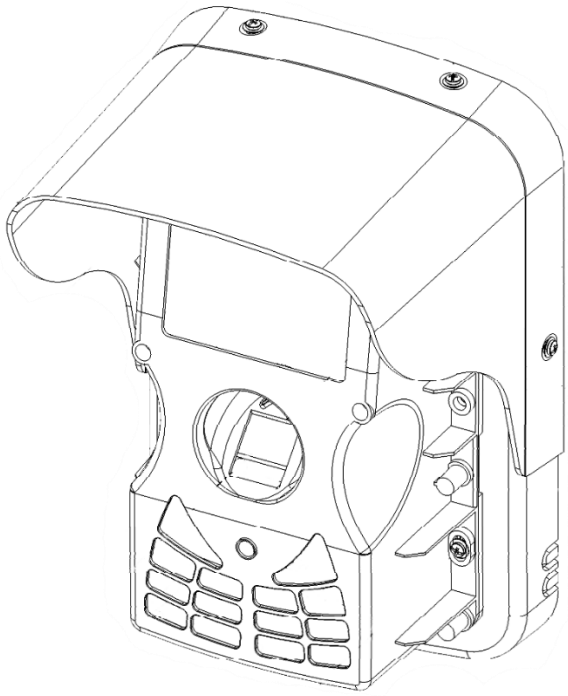
SECTION 6
INSTALLATION GUIDELINES

When correctly installed, your iPB7 biometric device is rated as an IP65 unit. For more information on what this means, please see Appendix A – Understanding IP Ratings.

If you are mounting your device outside, it is best to use the specifically designed mounting plate and rain cover, available as an optional extra, to ensure that your device receives maximum protection from the elements.

Below are images of what the iPB7 device looks like with the optional mounting bracket and the rain cover installed.





An iPB7 was designed to be exceptionally easy to install and maintain. We are going to explore installing the device both with, and without, the optional mounting bracket and rain cover. In either case, it is important to remember that you should wire up all your connectors and the IntelliRelay™ first before installing your device to ensure that the cable from the IntelliRelay™ is available at the point of installation and already connected to the all the relevant network points, power sources and devices to ensure that your iPB7 functions according to specification.

Installation WITHOUT optional bracket and rain cover

Installing the iPB7 biometric device without its optional mounting bracket and rain cover is extremely simple. Take the iPB7 biometric unit and connect it to the IntelliRelay™ via the Cat 5 cable as explained in Section 2. Once the cables are in place, and connected, simply use the provided 3 mounting holes on each side to screw the iPB7 device to the wall. Remember to ensure that the device uses at least 4 of the provided holes to ensure stability, and preferably, use all 6 of them if circumstances allow.

Figure 9 - iPB7 mounting holes

Once this has been done, and the device is snugly fitted to the wall, you can clip on the provided front cover, which will hide all the screws.

Figure 10 - iPB7 Front Cover

To remove the front cover, squeeze the sides of the unit, towards the centre, and use a screwdriver to edge up and unclip the front cover from the actual iPB7 device. Be careful not to scratch or damage your front cover when doing this, which is very easy to do. You should hear a click and feel the unit come loose once you have successfully disengaged the front cover from the unit.

Installation WITH optional bracket and rain cover

When installing the iPB7 biometric device on a hard surface (not a partition or wooden wall), or when installing the device outside, it is highly suggested that you use the mounting bracket and (if required) rain cover to simplify your installation and protect the device.

The diagram below shows how to install the unit in this situation:

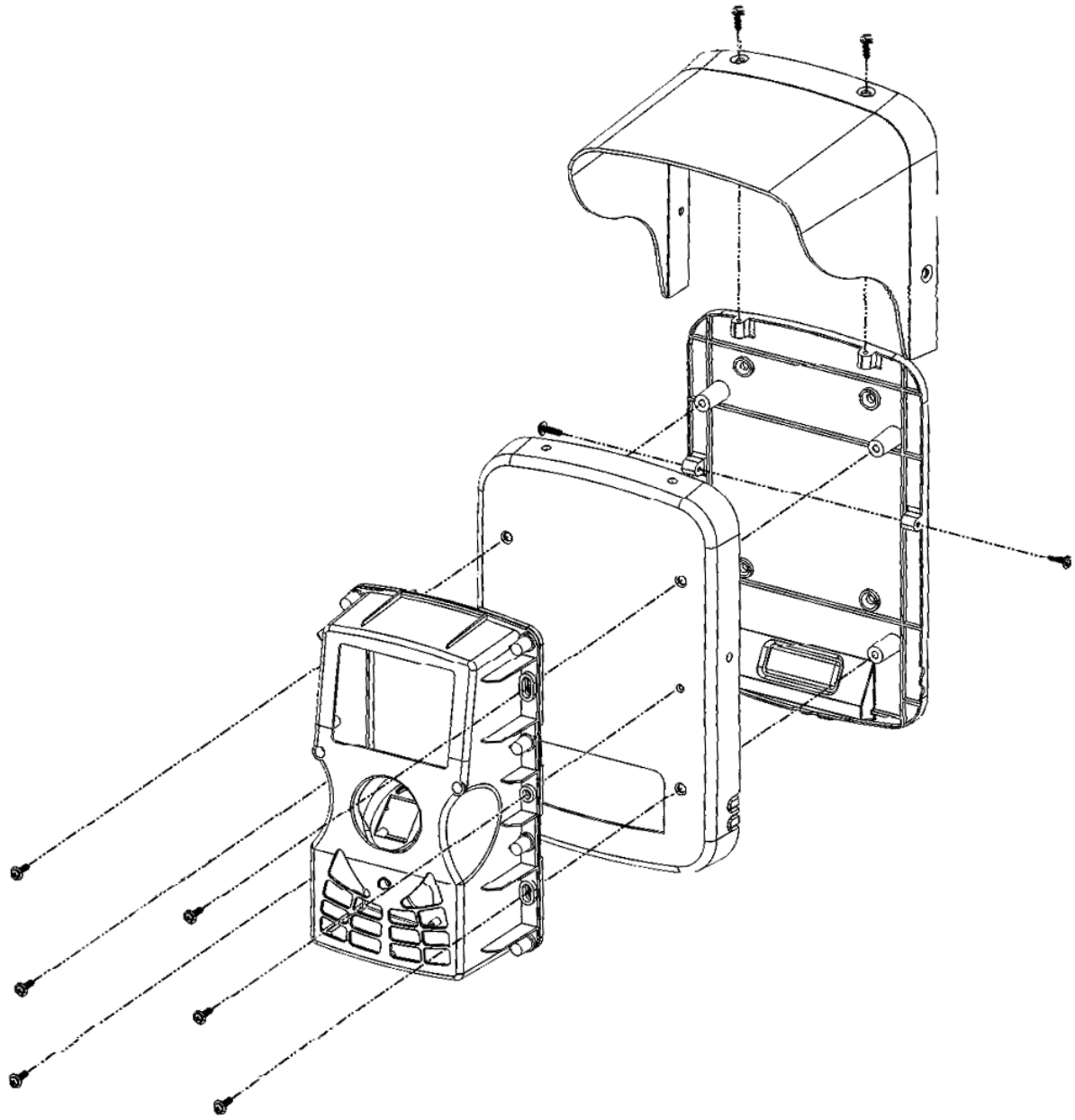


Figure 11 - Installing an iPB7 with bracket & rain cover

One of the significant benefits of installing using the mounting bracket is the ability to pre-mount the backing plate, thus allowing for all cabling to be installed prior to finishing off painting or repairing the walls if required. The mounting cover with the iPB7 biometric device attached, can then be easily installed afterwards with no damage caused in any way.

SECTION 7
CONFIGURING YOUR DEVICE

Your iPB7 biometric device was designed to be extremely simple to configure and use. Depending on which of the software applications you use to manage your device, there is very little to do to get it up and running.

Connecting it to the IntelliRelay™ and having the IntelliRelay™ connected to the network is normally all that is required for your reader to identify itself to the software, and to be ready to install. iPulse calls this auto-identification the **zero-configuration mode (ZCM)** and it is a unique feature of the iPBx range of biometric readers. This is when the unit is being used with the **IQSuite.cloud** software.

On booting, your iPB7 biometric device will issue several beeps, as well as displaying an iPulse logo during the boot up sequence. Once it is successfully booted, you should see the following screen:

Figure 12 - iPB7 Rest Screen

The two icons on the bottom left of the screen represent the following:

A GREEN circle with a cloud inside of it means that the unit has successfully connected to the Internet, or, in the case of a local server solution being implemented, to the local host or server.

A RED circle with a cloud inside of it means that the unit has been unable to connect to the Internet, which means that it will not be able to function without intervention from your IT team or installer. See the ***GETTING YOUR IPB7 ONLINE*** troubleshooting box later in this chapter for more information.

A GREEN circle with the letters IQ inside of it is the best possible sign. It means that your iPB7 biometric device is on the internet and has successfully connected to the **IQSuite.cloud** server software. You are good to go!

A RED circle, when combined with a RED cloud, is very common. This means your unit is not connected to the Internet and is thus unable to connect to the **IQSuite.cloud** server software. When combined with a GREEN cloud, this means that your unit is either incorrectly configured, or that your server is offline.

Under some circumstances, there may be additional icons at the bottom of the screen, to the right of the Internet and **IQSuite.cloud** icons. These icons represent mobile network connectivity, and GPS signal, when the iPB7 is connected to a modem that is supplied by iPulse with custom firmware.

The following icons reflect the signal and status of the GSM network, as follows:

The first orange circle means that there is signal, but extremely poor and that it may not be successful in uploading live clocks. From 2 to 5 bars are standard signals that represent signal strength, from low to high.

The red circle means that the unit is unable to find a GSM data signal, and therefore cannot connect.

The following icons represent the signal and status of the GPS or satellite network, as follows:

The green signal represents perfect GPS reception, and indicates that it is getting live GPS coordinates from the modem. The orange signal indicates that it HAS GPS coordinates, but that they are more than 8 minutes old. The red signal indicates that it has not received a GPS coordinate update for more than 16 minutes and will therefore no longer append GPS coordinate to the clock.

Under some circumstances, and if the device has been configured for use with a system other than **IQSuite.cloud**, the IQ symbol may be replaced with the specific symbol representing that company's software.

For example, when integrated with Comb Communications, the IQ symbol will reflect the following icons instead of the IQ icons:

In this case, the success of the connection to the Comb Portal is indicated in the same manner as **IQSuite.cloud** where green represents a successful connection, and red that it has not successfully connected.

To configure your device with other systems and software, please check the relevant products user manual, as many of these systems have different versions of firmware, or different implementations and thus different solutions to problems.

In these cases, the supplier of the software will often provide a software tool or mechanism to change the iPB7 to work with their software, and in some cases, devices will come pre-configured and can only be used if purchased from that specific supplier.

Please check carefully what the policy is before purchasing iPB7 devices for use with other platforms to ensure that you do not end up paying again for a license or service fee to have it linked to your specific software.

GETTING YOUR IPB7 ONLINE WITH A FIREWALL

*There are a few simple tricks to check if your iPB7 has successfully connected to the Internet. Your iPB7 is configured to use **DHCP by default**, so if you connect the network cable to a network that has both internet connectivity and a DHCP router, you should be up and running first time.*

If your iPB7 is unable to get onto the network, you may require a static IP address, or some additional networking information. This can be supplied by your internal network team, and your reseller or approved installer can use the iPulse Config Tool to enable these settings.

Firstly, the **OUTGOING PING** *option needs to be enabled on your firewall. Without this, the iPBx devices will assume that the network is offline, as they use the PING command to establish connectivity.*

*One of the main causes of your iPB7 not getting online in large organisations is the firewall. You should always make sure that the following ports are open on your firewall to allow the iPB7 to communicate with the **IQSuite**.cloud server:*

Port 80 – HTTP

Port 443 – HTTPS

Port 53 – DNS

Port 123 – NTP

With these four ports open, your iPB7 should have no problem communicating on the network. Also, it is important to remember that if you want remote support and assistance from iPulse Systems at some stage, they will need you to open the following additional port to ensure that they can communicate with the readers remotely:

Port 22 - SSH

SECTION 8
IQSUITE AND OTHER SOFTWARE

The configuration and use of your iPBx Biometric Device is dependent on the type of software you are using. All iPBx devices are compatible with the iPulse **IQSuite.cloud** software system, both in the hosted or local environments, and are configured to work out of the box in what is known as a **zero-configuration mode (ZCM)**. ZCM is currently only available when using the iPBx through the **IQSuite.cloud** platform.

When using your iPBx biometric device with **IQSuite.cloud**, you will not need to do anything other than to ensure that the iPBx is connected (via the IntelliRelay™) to the local network, is able to receive an IP address and gateway from the local DHCP server and is able to access the internet.

Thereafter, you may follow the **IQSuite.cloud** manual for further details of how to connect the device to the software and configure it from there.

However, there are many other software solutions available, including the following:

- **IQSuite** 4.4x (iPulse Systems)
- XTime (G4S Secure Solutions)
- Smart Time (Page Automation)
- Jarrison Time (Jarrison Systems)
- Comb Portal (Comb Communications)

For more information on how to configure your device with each of these platforms, or with **IQSuite.cloud** platform, please visit http://www.iqsuite.cloud and download the relevant manual. You will also find a wealth of updated information on which software systems support the iPBx out of the box, and how to use or configure your iPBx to work with these solutions.

SECTION 9
CARING FOR YOUR IPB7

Although iPulse Systems biometric devices are built to be tough as well as capable, taking good care of your device will most certainly help in ensuring that it enjoys a longer operational lifespan.

GENERAL GUIDELINES

- iPB7 biometric devices are NOT waterproof, although they are highly resistant to weather. If the device is to be mounted outside, try to ensure that it has been protected as much as possible from the elements, either under a cover or mounted in such a fashion that it does not get exposed.
- Using the specifically designed mounting bracket and rain cover – supplied as optional extra's on request – will significantly enhance the longevity and weather proofing of your iPB7 device.
- Where possible, the iPB7 biometric devices should not be mounted in direct sunlight. The fingerprint sensor can heat up and burn your finger if it gets too hot. This can also cause the components to overheat, as well as cause damage to your casing, which could fade or discolour over time. In extreme cases, the screen has also been known to turn black when the ambient temperature reaches above 45°C (113°F), although it returns to normal functionality when the unit cools down again.
- Always ensure that your iPB7 biometric devices stay within operational temperatures specified. Using the device in temperatures lower than 0°C (32°F) or above 45°C (113°F).
- You should avoid allowing your iPB7 biometric device to come into contact with corrosive materials, which can damage your casing, and in extreme conditions, significantly damage the electronics.

CLEANING YOUR IPB7

Should you wish to wash or clean your iPB7 biometric device, please keep the following guidelines in mind:

- Cleaning substances should never be sprayed directly onto the device, but rather, applied to a rag or cloth, and then used to wipe off any dirt or grime.
- The following products may NOT be used under any circumstances to clean your device, as use of these products may damage not only the casing, but also, the electronics or the fingerprint sensor:
    - Paint thinners
    - Acetone
    - Methylated spirits
    - Bleach
    - Any oil-based product

APPENDIX A
UNDERSTANDING IP RATINGS

First Digit: Protection against Solids

Level	Protection Against	Description
0	-----	No Protection
1	Solid objects > 50 mm	Back of a hand; no protection against deliberate contact with a body part
2	Solid objects > 12.5 mm	Fingers or similar objects
3	Solid objects > 2.5 mm	Tools, thick wires, etc.
4	Solid objects > 1 mm	Most wires, screws, etc.
5	Dust Protected	Ingress of dust not entirely prevented, but does not interfere with operation of the equipment
6	Dust Tight	No ingress of dust, complete protection against contact

Second Digit: Protection against Water

Level	Protection Against	Description
0	-----	No Protection
1	Dripping water	Vertically falling drops have no harmful effect
2	Dripping water when tilted up to 15°	Vertically falling drops have no harmful effect when enclosure is tilted at an angle up to 15° from its normal position
3	Spraying water	Water falling as a spray at any angle up to 60° from the vertical has no harmful effect
4	Splashing Water	Water splashing against the enclosure from any direction has no harmful effect
5	Water Jets	Water projected by a nozzle against enclosure has no harmful effect
6	Powerful Water Jets	Water projected in powerful jets against enclosure has no harmful effect
7	Immersion up to 1m	Ingress of water in harmful quantity when enclosure is immersed in water (up to 1 m of submersion)
8	Immersion beyond 1m	Depends on the specification of the manufacturer. Equipment may be hermetically sealed or it means that a certain amount of water can enter the enclosure without harmful effects

APPENDIX B
IPB7 MESSAGING

When the iPB7 displays this screen, you have successfully configured your device, and it is both on the Internet, and successfully connected to the **IQSuite.cloud** file server.

In this instance, your device is ready to go.

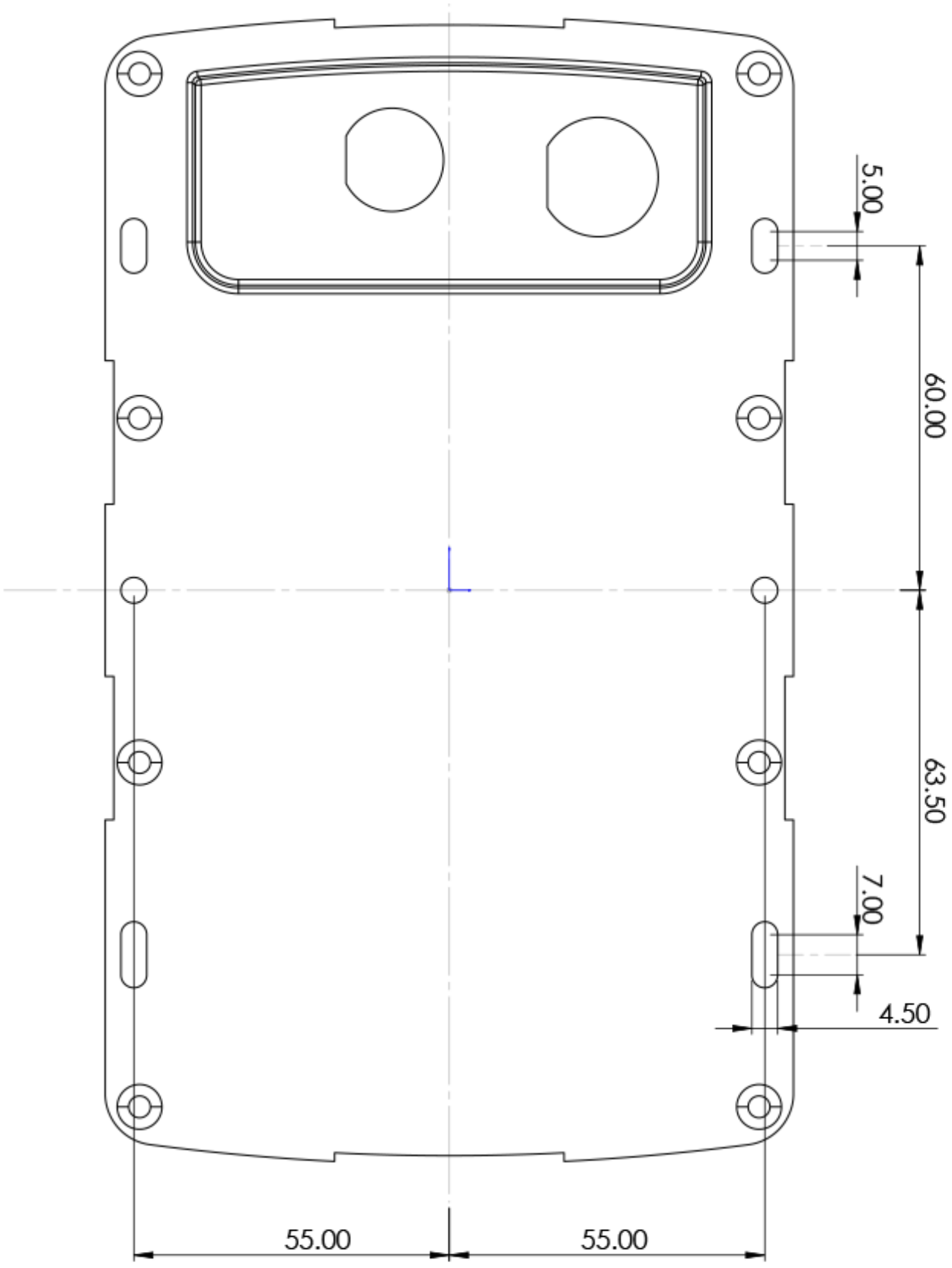
When the iPB7 displays this screen, your device is not connected to the Internet, and thus is unable to connect to the **IQSuite.cloud** server.

See Section 7 for more information about how to troubleshoot this situation.

When the iPB7 displays this screen, your device has successfully connected to the Internet, but is unable to connect to the **IQSuite.cloud** server.

The two main causes of this are that the device is not correctly allocated to your specific instance of **IQSuite.cloud** server, or that your instance of the **IQSuite.cloud** server is currently offline.

APPENDIX C
IPB7 MOUNTING TEMPLATE



APPENDIX D
IP65 INSTALLATION TIPS

1

Weather shield
Although the device is IP65 rated, additional protection against liquid ingress (especially rain) will significantly extend your device's lifespan.

2

Mounting the reader flush
When installing an iPB7, mount the reader flush with the mounting surface. Take special care to ensure that liquids don't seep in behind the reader and the surface or if it does, that the liquid has a means of escape. Liquid pooling in the connector cavity is akin to the connectors being submerged, something the device was not designed for. This is easily achieved by using the specially designed iPB7 mounting bracket and rain cover, available as an optional extra.

3

Use grommets
Grommets can be used to cover the connectors at the rear of the device. Take special care to tighten and secure these properly. These grommets are available from most cable suppliers, and also from iPulse on request.

4

Mount under cover
If a device is mounted without a weather shield, it is advisable to install where it is shielded from the elements by a roof, overhang or similar to protect it from as many environmental factors as possible. Where possible, try to use the iPulse rain cover, supplied as an optional extra on request.

5

Do not wash the device
When cleaning your device, wipe it down with a dry or damp (not wet) cloth. Pressure washers, hoses and the like may damage the device and should be avoided. The reader should be installed out of reach of sprinklers.

APPENDIX E
INTERPRETING CLOCK TYPES

ClockID	Name	Description - Database & Reader
0	AccessGranted	Access Granted
1	AccessGrantedPIN	Access Granted - PIN Only
2	AccessGrantedCard	Access Granted - Card Only
3	PersonNotIdentified	Access Denied - Unidentified Person
4	PersonFileNotFound	Access Denied - Record not Found
5	BeforeCommenceDate	Access Denied - Prior to Commencement
6	AfterExpiryDate	Access Denied - Access Expired
7	OutsideScheduledTime	Access Denied - Outside Schedule
8	TokensExpired	Access Denied - Tokens Expired
9	RescanDelay	Access Denied - Time Delay
10	PinNotFound	Access Denied - PIN Not Found
11	PinFingerMismatch	Access Denied - PIN/ Finger Mismatch
12	AccessGrantedBreath	Access Granted - Breathalyzer Passed
13	DeniedPINNoFinger	Access Denied - PIN Without Finger
14	FailedBreathalyzer	Access Denied - Breathalyzer Failed
15	BreathalyzerTimeOut	Access Denied - Breathalyzer TimeOut
16	NoPrintCardUser	Access Denied - No Print
17	PrintCardMismatch	Access Denied - Card/ Finger Mismatch
18	AccessGrantedWiegand	Access Granted - Wiegand Controller
19	AccessDeniedWiegand	Access Denied - Wiegand Controller
20	WiegandTimeOut	Access Denied - Wiegand Time Out
21	CardNotFound	Access Denied - Card Not Found
22	ReaderInactiveDenied	Access Denied - Reader Inactive
23	PersonInactiveDenied	Access Denied - Person Inactive
24	RelayDoorClosed	Event Log - Door Closed
25	RelayDoorOpened	Event Log - Door Opened
26	RelayDoorLocked	Event Log - Door Locked
27	RelayDoorUnlocked	Event Log - Door Unlocked
28	AccessGrantedPanic	Access Granted - PANIC Finger
29	AccessGrantedAuth	Access Granted - Authorized
30	AccessDeniedAuth	Access Denied - Not Authorized
31	AccessDeniedAuthTO	Access Denied - Authorization TimeOut

APPENDIX F
UNDERSTANDING FINGERPRINTS

FINGERPRINTS: A BRIEF OVERVIEW

One of the most common questions surrounding fingerprint biometrics is whether or not we store an actual image of the fingerprint. The simple answer is no! The data is extracted using an algorithm, unique to each company. An algorithm is a step-by-step procedure for calculations, used for data processing and automated reasoning.

In this instance, the algorithm extracts identifying points, known as minutiae, from the image of a person's fingerprint. These points, based on the patterns found on the fingerprint, are mapped as a series of data points called a **minutiae string**. A **biometric template** is constructed from at least two minutiae strings, and this what gets stored for later use in a database or on a device.

BASIC PATTERNS

Fingerprints usually consist of one of three basic patterns:

- **Arch**: Ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger.
- **Loop**: Ridges enter from one side of a finger, form a curve, and then exit on that same side.
- **Whorl**: Ridges form circularly around a central point on the finger.

A fingerprint can also combine more than one pattern of the same or differing types, such as a double-loop or a two deltas that accidentally form a whorl.

On average, roughly 65% of the population have loops, 30% have whorls and only 5% have arches.

Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns can be inherited[i].

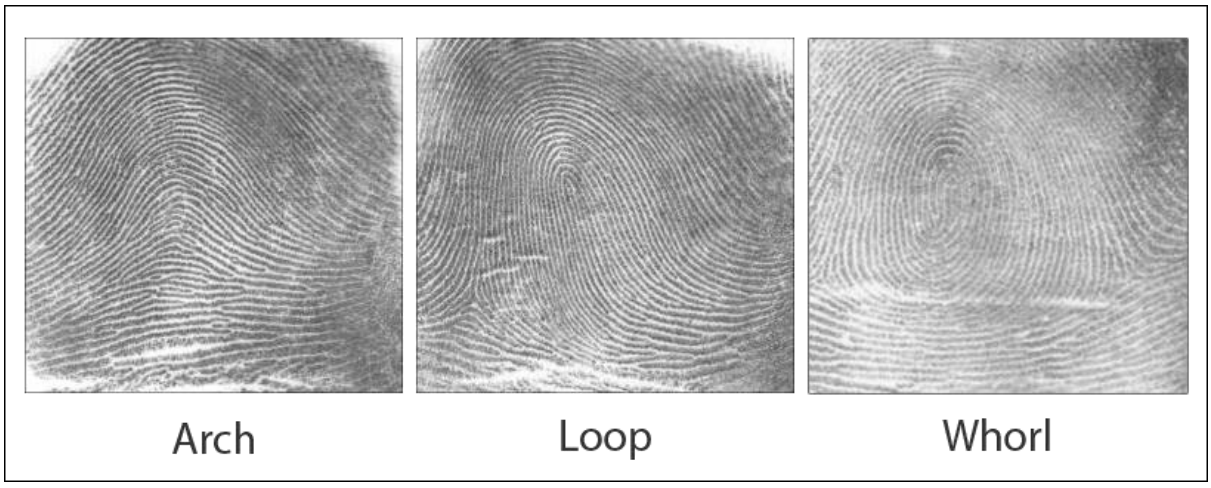


Figure 13 - Common fingerprint Types

MINUTIA

Minutia points are the major defining characteristics of a fingerprint. When a fingerprint is analyzed, each minutia point is marked and mapped in relation to other minutia points as well as its general location in the fingerprint.

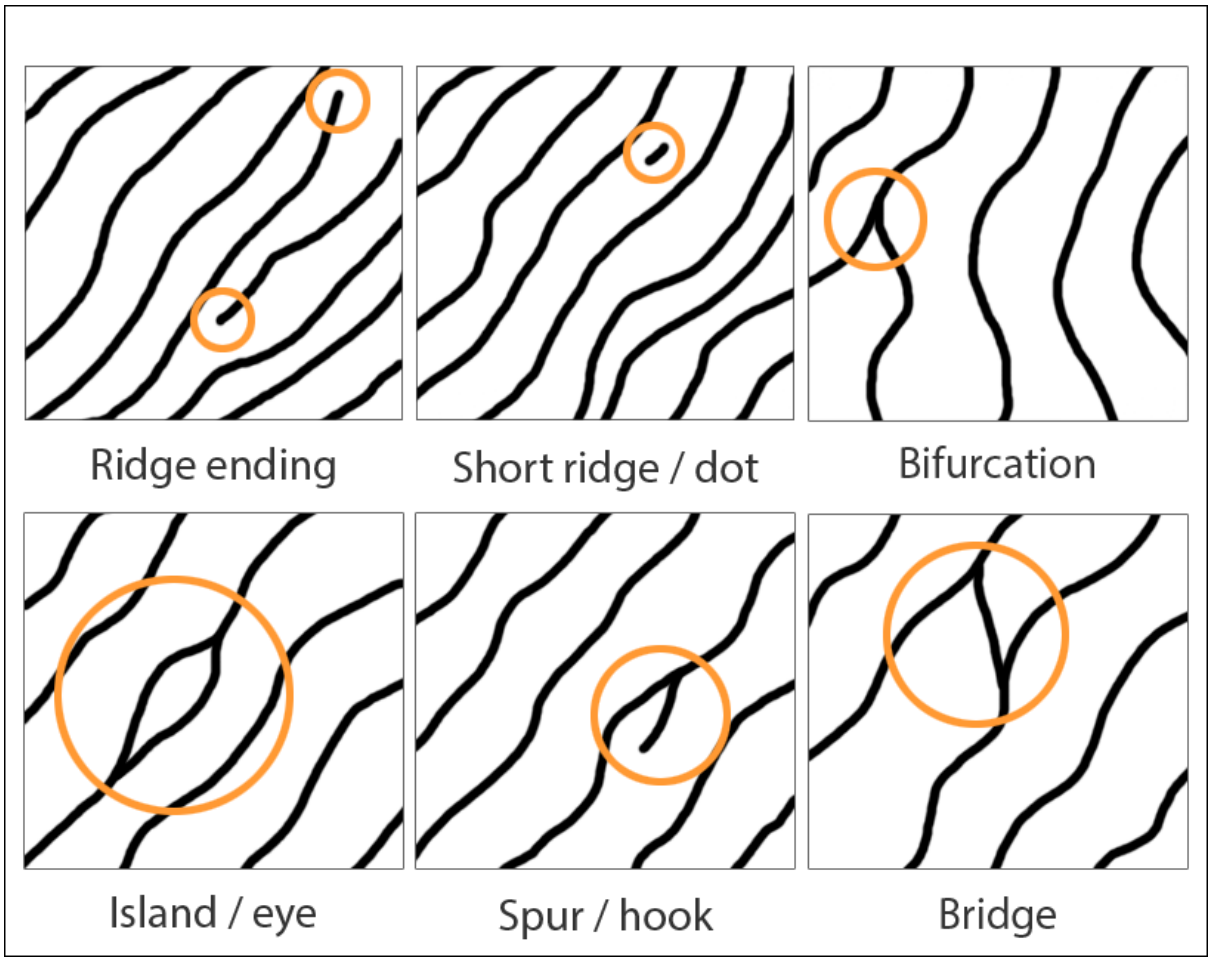


Figure 14 - Common minutia points

Common Minutia Points

- **Ridge ending** – a point where the ridge terminates.
- **Short ridge or dot** – ridges with a significantly shorter length than the average ridge length on the fingerprint.
- **Bifurcation** – points where a single ridge splits into two ridges.
- **Island or eye** – a point where a single ridge splits into two before converging into a single ridge again.
- **Spur or hook** – a shorter ridge terminating soon after it branched from its originating ridge.
- **Bridge** – a short ridge that connecting two larger ridges. It can also be seen as two bifurcating ridges that share a common branch.
- **Core** – a ridge that bends back on itself or forms a U-turn.

THE FINGERPRINT ENROLLMENT PROCESS

Now that we understand the identifying features in fingerprints, let's take a look at what happens behind the scenes when a biometric template is constructed.

Note: *iPulse makes use of SecuGen's optical sensor technology. For the purposes of this document, explanations are based on the use of these particular devices.*

Before we can proceed, we need a digital image of the fingerprint. When a finger is placed on the biometric scanner's touch plate, a visible light, commonly red, is shined on the fingerprint through a clear prism. The reflected light from the fingerprint is picked up by the optical sensor *(an optical biometric device is, essentially, a highly-specialized digital camera)* in the device and a digital image is created.

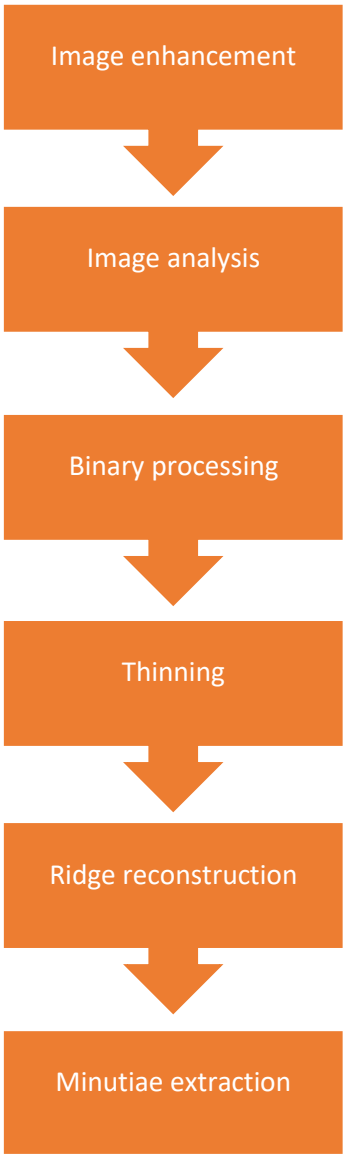


Figure 15 - Fingerprint Enrolment Process

IMAGE ENHANCEMENT

Before we can analyze the image, we need to clean it up a little: reduce noise, sharpen and enhance the difference between ridges and valleys in the image, optimize the contrast and generally improve the image quality as much as we can.

Figure 16 - Base to Enhanced Images

IMAGE ANALYSIS

Using the enhanced image, we move to analysis. In this step, we select the background region to mark smeared or smudged regions which shouldn't be used as part of the template. Once those have been isolated, we split the image into blocks and determine their direction.

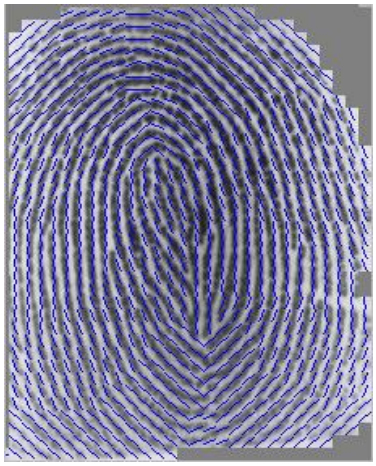


Figure 17 - Analysed image with background and smudges removed

BINARY PROCESSING

Analysis complete, we carefully convert the image to binary. To do this, the grayscale image is converted to a black and white image. Once in black and white, the image can be digitized into ones and zeroes, as shown in the images below.

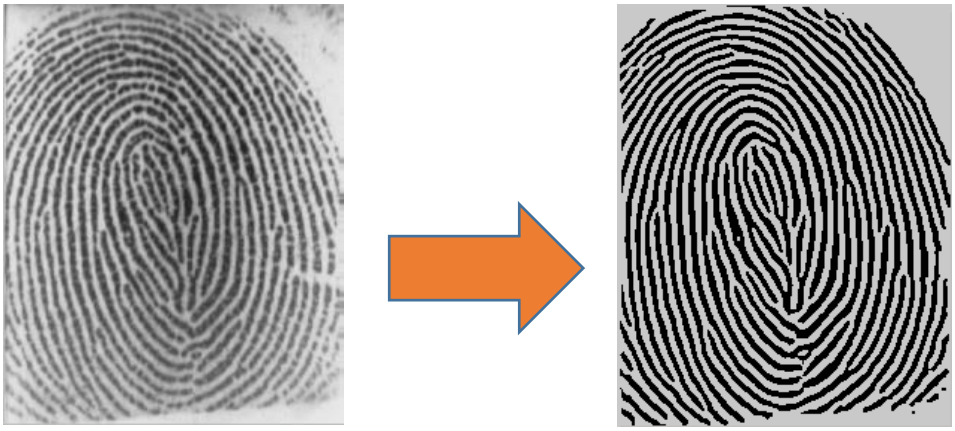


Figure 18 - Enhanced to Digitized Images

THINNING

Digitizing complete, the image is cleaned some more. All ridges are thinned down until they are no more than a single pixel wide. This allows much easier identification of the overall shape of the print.

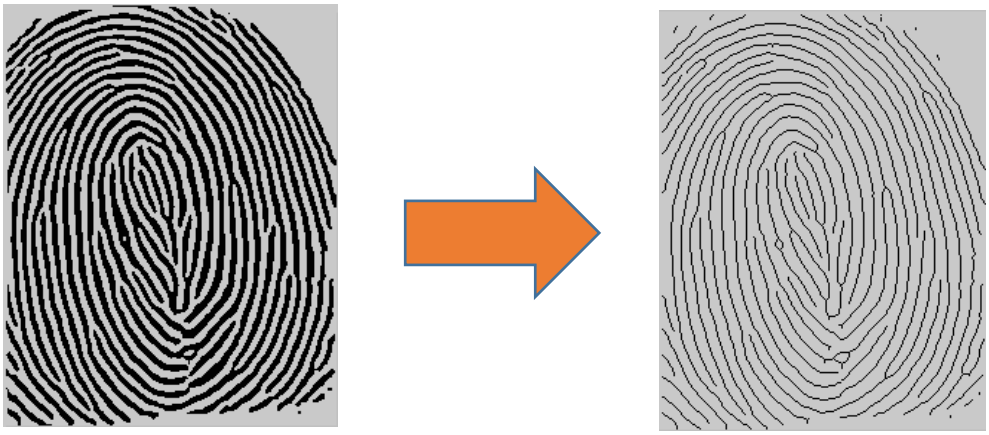


Figure 19 - Digitized to Thinned Images

RIDGE RECONSTRUCTION

Now that we've got the image in its most basic format, we can start a process known as **Ridge Reconstruction.** During this process, we eliminate a number of interferences like **spurious fusions** – multiple joining points - and a**ir bubbles and islands** – little ovals in the print lines – before we rejoin any cuts that have occurred and remove remaining fake ends.

The image on the right shows an example of a reconstructed image:

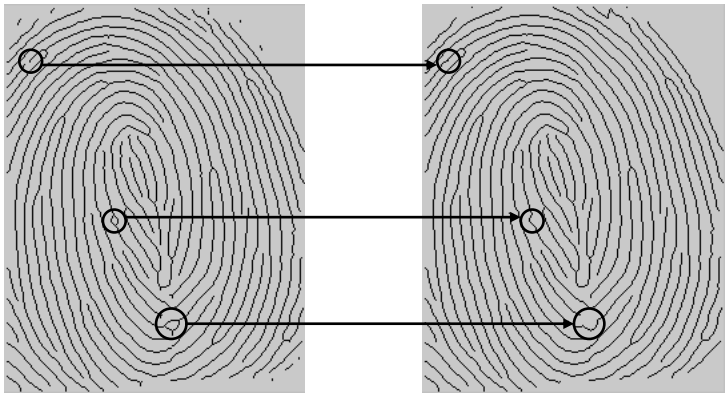


Figure 10 - Ridge reconstruction

MINUTIAE EXTRACTION

A highly complex mathematical formula, part of what differentiates each manufacturer's algorithm from others, is used to classify fusions and endings, their directions and relative locations to each other. When the algorithm has mapped all these points, it builds the final template: the minutiae string that uniquely identifies this fingerprint. To the eye, this looks like nothing more than a long string of random numbers.

The image below shows the overall progress – from the base image we started with to one where the minutia points and their directions as an overlay on the original. This is what the information looks like before the final minutiae string is built.

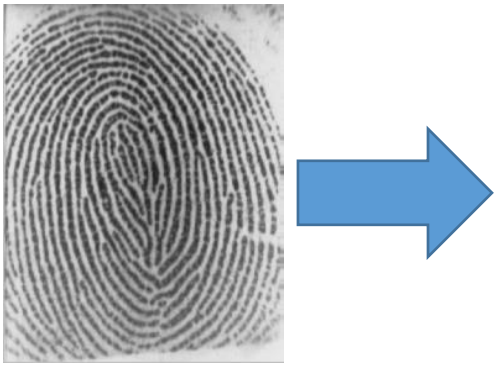


Figure 11 - Base image

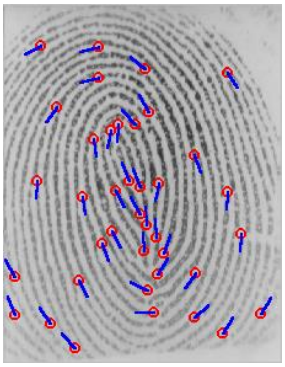


Figure 12 - Base image with the minutia points and directions overlay

On this image, each red dot represents a minutia point. The list to the right shows the numeric location of each of these points, which will, eventually, become the minutiae string data.

MEASURING PERFORMANCE ON BIOMETRIC SYSTEMS

Measuring the actual performance of a biometric system is a complex process affected by various factors, including – but not limited to – environmental conditions, human interference and incorrect, sometimes conflicting system settings.

Fingerprint-based biometric devices allow manual changes to the threshold at which a print is deemed an accurate enough comparison to be considered a successful match. With a low threshold – for example, only 10% of the minutiae points need to be matched for a "successful" identification – very few people will experience trouble being identified by the system. The drawback to this, however, is an increased risk in possible "false" identifications.

Raising this threshold holds true for the opposite: with a higher number of minutiae points required for a successful match, chances are increased that people will not be identified by the device. At the same time, the risk of someone being identified as someone else drops quite significantly.

The ideal is a balance between these two extremes, a setting where the threshold for successful matches is high enough to avoid false identifications, yet low enough to match people consistently and without difficulty. These settings can be changed dynamically according to the requirements of the situation.

CORE METRICS

In general, three core metrics are used to determine the performance of a biometric system.

False Rejection Rate (FRR)

Also referred to as **False Non-Match Rate (FNMR)**, this indicates the probability that the system will fail to detect a match between the input pattern and a matching stored template. It measures the percentage of valid inputs that are incorrectly rejected.

False Acceptance Rate (FAR)

Also referred to as **False Matching Rate (FMR),** this indicates the probability that the system will incorrectly match the input pattern to a stored non-matching template. It measures the percentage of invalid inputs which are incorrectly accepted.

Equal Error Rate (EER)

Also referred to as **Crossover Error Rate (CER),** this indicates the rate at which both false acceptances (FAR) and false rejections (FRR) errors are equal; i.e. for each false acceptance there will be one false rejection. The EER is a quick way to compare different biometric systems – the system with the lowest EER score is the most accurate.

CERTIFICATION AUTHORITIES

The first two metrics (**FRR** and **FAR**) are usually published by the **International Biometrics Group (IBG),** a for-profit biometric industry organisation that performs these tests. There are, however, several deficiencies and shortcomings in the IBG tests, the most crucial of which is that all tests are performed in laboratory conditions with a relatively small sample database.

The **American National Institute of Standards and Technologies (NIST)** is the only internationally well-respected, neutral third party that performs independent tests on fingerprint capture devices. This organisation uses a standard database of images and standardised procedures on fingerprint-based biometric devices to determine the FAR, FRR and EER rates, bestowing a **Minutiae Interoperability Exchange** or **MINEX** certification based on performance.

THE MINEX CERTIFICATION

The MINEX certification exists to

- Provide measurements of performance and interoperability of core template encoding and matching capabilities to users, vendors and interested parties.
- Establish compliance for template encoders and matchers for the United States Government's **Personal Identity Verification (PIV)** program.

The Secugen sensors and algorithms used in all iPulse biometric devices are rated as follows:

IBG: FAR 0%, FRR 0%
NIST: EER of 0.0042 and certified **MINEX** compliant

COMPARING FRR / FAR RATINGS ON FINGERPRINT, FACIAL AND VOICE BIOMETRICS

There are always questions relating to the different biometrics available - fingerprints, facial, voice etc. – and how they compare. Different studies have been conducted with a focus on the FRR and FAR rates. The table below indicates the outcomes of some of these studies.

	Test	Test Parameter	False Reject Rate (FRR)	False Accept Rate (FAR)
Fingerprint	FVC 2002*	Users mostly in the age group 20-39	0.2%	0.2%
Face	FRVT 2002**	Enrollment and test images were collected in indoor environment and could be on different days	10%	1%
Voice	NIST 2000***	Text dependent	10-20%	2-5%

*Fingerprint Verification Competition; bias.csr.unibo.it/fvc2002
**Face Recognition Vendor Test; www.frvt.org/FRVT2002
***National Institute of Standards and Technology; www.nist.gov/speech/tests/spk/2000

The manner in which a match is obtained can make a large difference to the perceived performance of a biometric system.

1:N (ONE-TO-MANY) MATCHING

One-to-Many matching is another name for the process of identifying an unknown person from a provided biometric credential like a fingerprint. Once the person has placed his/her finger on a sensor, the provided biometric sample is matched against each stored biometric template on the device / in the database.

If no such template matches the sample, no data is returned. If a matching template was found, the identity linked to it will be returned.

Benefits

- Simple to use – a biometric sample is all that is required.

Drawbacks

- Can be slow – depends on number of templates to match against and the efficiency of the algorithm used.
- Higher chance of false rejections and false acceptances
- Only a single factor on which authentication will be based.

1:1 (ONE-TO-ONE) MATCHING

One-to-One matching is another way of referring to the process of verifying that the provided biometric sample matches a single, specified identity. Because we know which identity we're looking for, we don't need to match against every stored biometric – we take the provided sample and compare it directly to the biometrics linked to the specified identity. The result will be the acceptance or refusal of the identity claim.

The term 'verification' was defined in a previous draft of the Harmonized Biometric Vocabulary document as a 'one-to-one process of comparing a submitted biometric sample (…) against the biometric reference template (…) of a single enrolee (…) whose identity is being claimed, to determine whether it matches the enrolee's template'. Contrast with identification (…)".

Benefits

- One-to-One matches are much faster than One-to-Many matches.
- Because we know which biometric template the provided sample needs to match, we can lower the matching threshold to allow a better chance of a match being detected.
- Significantly lower chance of false acceptances and false rejections.
- Multi-factor authentication offers better security with each additional factor.

Drawbacks

- The person may forget or lose a card
- The person may forget a PIN code

MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (**MFA**) is an approach to authentication which requires the presentation of two or more authentication factors of the following kind:

- **A knowledge factor:** something only the user *knows*, like a PIN or password.
- **A possession factor:** something the user *has*, like an ID card or NFC tag.
- **An inherence factor:** something the user *is,* a biometric characteristic such as a fingerprint.

A one-to-one matching system based on multi-factor authentication significantly increases the security of your system while lowering false acceptance and rejection rates. Presenting a smart card to a device capable of reading it, for instance, immediately satisfies the possession factor and tells the system exactly which identity we wish to confirm. By placing a finger on the biometric reader, the inherence factor is met and a 1:1 match can be done. We now have two levels on which we can authenticate the person's identity:

- Has the person presented a recognized card?
- Does the fingerprint match the identity linked to the card?

APPENDIX F
ENROLLMENT GUIDE

A QUICK GUIDE TO ENROLMENT

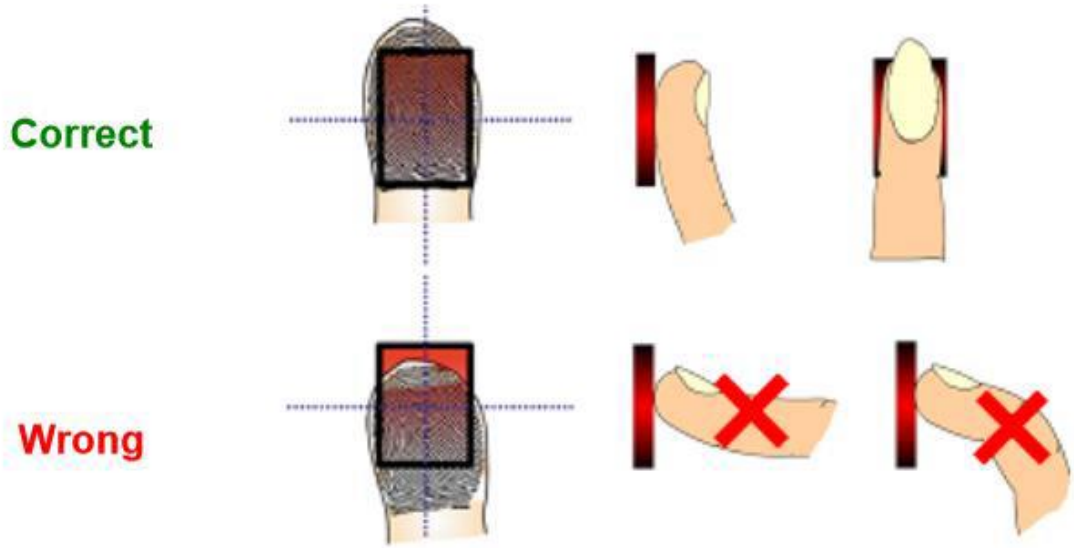
It is important to keep in mind that the enrolment process is the most important part of the user's experience. Capturing better prints at the time of enrolment will increase the user's experience when using the rest of the system for life.

The iPulse **IQSuite Cloud 5.0** software system has one of the most comprehensive and easy to use enrolment processes in the world, clearly help you to visually understand the quality of the print you have captured.

When capturing a fingerprint, there are a few important rules to keep in mind:

- Don't tap – Place your finger down firmly and keep it there until a print is captured.
- Don't hover – Do not hover slightly above the sensor, be assertive.
- Don't slide – Do not slide you finger onto the sensor, simply put it down firmly.
- Cold fingers – Always try to warm your hands and fingers before capturing prints.
- Dry fingers – Always try to have a little moisture or oil on your fingertips.

The user should put their finger down firmly in the center of the sensor and keep it there until the image is captured. It is advised that the user do it multiple times to ensure they are comfortable using a fingerprint reader. Below are some guidelines that will help with finger placement to ensure the best quality capture.



APPENDIX G
POE & ACCESS CONTROL

POWER OVER ETHERNET: A BRIEF OVERVIEW

Power over Ethernet (PoE) is a technology for wired Ethernet LANs (local area networks) that allows the electrical current necessary for the operation of specific devices to be carried over the data cables, thus negating the need to have power at the end point of installation.

The concept behind this is to minimise the number of wires required for an installation. From a cabling perspective at least, the end result is lower cost, easier maintenance, and greater installation flexibility than with traditional wiring methods.

For PoE to work, the electrical current must go into the data cable at the power-supply end, and come out at the device end, in such a way that the current is kept separate from the data signal so that neither interferes with the other.

The current enters the cable by means of a component called an injector. If the device at the other end of the cable is PoE compatible, then that device will function properly without modification. If the device is not PoE compatible, then a component called a picker or tap must be installed to remove the current from the cable before being connected to the device. This "picked-off" current can then be routed to the power jack.

POE STANDARDS

The IEEE standard for PoE requires category 5 cable or higher for high power levels. Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a mid-span power supply.

The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350 mA to each device.

The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power (minimum 44 V DC and 575 mA. The 2009 standard prohibits a powered device from using all four pairs for power.

DEVICES TYPICALLY USED WITH POE

PoE provides both data and power connections in one cable, so equipment doesn't require a separate cable for each need. For equipment that does not already have a power or data connection, PoE can be attractive when the power demand is modest. For example, PoE is useful for IP telephones, wireless access points, cameras with pan tilt and zoom (PTZ), and remote Ethernet switches.

DOWNSIDE OF POE WITH BIOMETRICS

However, it is important to note that there are some significant potential downsides to PoE installations, most specifically related to biometric installations.

PRINCIPLES OF ACCESS CONTROL

Since most biometric readers are used to manage access in secure areas, it is considered good practice to ensure that all readers are powered from separate battery backup units. This way, in the event of a power failure of some kind, only 1 or perhaps 2 devices are affected, rather than the entire setup.

With PoE, if the one central switch goes down, it can take down not only the communications, but the function of the access control units, across an entire wing or even an entire building.

MANAGING DEVICES

Another major disadvantage of biometric installations is that they tend to be connected to other devices such magnetic locks, striker locks and similar.

These devices tend to draw far more current than the biometric reader does, and most often, put significant strain onto the maximum allowed amperage being supplied by the device.

Experience has shown that whilst certain custom-made midspan devices can supply this current, their longevity is extremely poor, probably given that they do not follow the standards laid down for the maximum supply of power over Ethernet cables.

It is therefore critical that anyone using iPulse biometric devices with PoE should take great care to only use the recommended products to avoid issues with the continued successful operation of the system.

LIGHTNING AND CURRENT SURGES

In addition to the above, devices connected directly to the power supply are more susceptible to over voltage damage than those devices connected via a battery backup power supply, as the chances of the cable transmitting an overvoltage event such as a lightning strike are exponentially increased as the cable length increases.

USING POE WITH IPULSE BIOMETRICS

The iPulse iPBX range of biometric products currently does NOT natively support PoE, however, an updated IntelliRelay is expected during the course of 2018 that should support this.

However, in environments where the biometric reader is being used in isolation, such as a time and attendance reader NOT connected to any other devices, the use of PoE is possible, and extremely simple, if required.

CABLING AN IPBX READER TO WORK WITH POE

All the iPBX readers (with the exception of the iPB1 and iPB8 devices) are powered via the IntelliRelay. This device traditionally receives 13,8 V DC from a battery backup, and translates this power into that required for the reader.

In order to connect an iPBX reader to a PoE Ethernet cable, the best option is to purchase a splitter (also known as a “picker” or “tap”) which can be attached to the end of the PoE Ethernet cable sitting in the ceiling.

From this, you can then send the power to the IntelliRelay, and the network directly down to the reader, allowing your system to be powered from the central PoE switch.

RECOMMENDED PRODUCTS FOR USE WITH IPULSE IPBX PRODUCTS

As a market leader, iPulse Systems likes to partner with products that are well known for providing an excellent quality of service and reliability.

For this reason, iPulse Systems has elected to recommend PoE products from the worlds leader (and inventor) of PoE, Microsemi Corporation.

More information about Microsemi Corporation, and their range of products, can be found here.

The key products recommended for use when installing an iPBx device with PoE are the following:

Product Code	Description	Use Case
PD-AS-951/12	PoE Splitter	This is used to power an iPBx reader from a PoE cable
PD-3501G/AC	PoE Injector	This is a single port injector able to provide power from a central source over an Ethernet cable to a single iPBx device, and the associated locking mechanism.
PD-3504G/AC	PoE Injector	This is a four-port injector able to provide power from a central source over an Ethernet cable to up to 4 iPBx devices, and the associated locking mechanism.