PAC IEVO Configuration Manual

For PAC SecureNet/Access Central

Version 2.0 – June 2022

PAC IEVO Configuration Manual



Contents

1. Introduction

Utilising sophisticated optical sensors and advanced encryption for data transmission, IEVO Readers deliver a fast, accurate and reliable biometric solution to any business and industry.

This document is designed to provide a clear step-by-step guide to the configuration and operation of Revision 4, and earlier Revision 3, IEVO Biometric readers with PAC SecureNet access control software.

For further information on the Initial Installation and configuration of PAC SecureNet access control systems, please refer to the resources below.

Website: PACGDX.com

YouTube channel: https://www.youtube.com/c/PACGDX/videos

PAC Technical documents are available on request by contacting support@pacgdx.com

2. Pre-requisites

Software: PAC SecureNet version 4.6.422 or above (IEVO Revision 4)
Software: PAC SecureNet version 4.6.287 or above (IEVO Revision 3)
Licence: PAC SecureNet Lite or above
Hardware: PAC 512 Series Access Controllers (With Doors Configured)
Network: IP Network to facilitate communications between the PAC SecureNet server and IEVO modules.

IEVO Hardware as supplied by PAC, is specifically configured for use with PAC access control systems and as such, only PAC documentation should be followed during installation and commissioning of PAC IEVO products.

For the purpose of this document, it is assumed that SecureNet has already been configured in terms of Communication Channels, Controllers, Doors, Areas and Access groups. These topics are beyond the scope of this document; they are however covered in the SecureNet help files, which may be viewed in the **Help – Contents** section of the SecureNet tool bar**.**

Important note on IP configuration

It is strongly advised that all IEVO control boards are configured with the correct IP address, Subnet Mask and default gateway for the host network prior to physical installation. Failure to do so may result in the SecureNet Server being unable to communicate with the IEVO control board. If you are unsure of the correct IP settings, please consult the local Network administrator.

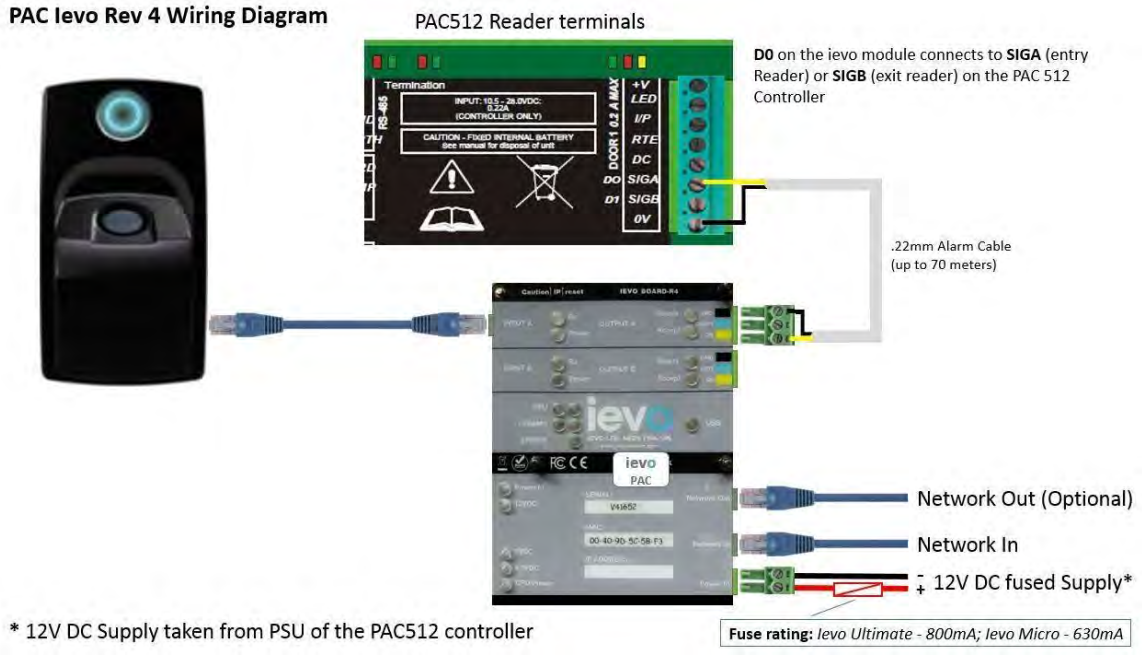
Important note Reader Data Voltage

For use with IEVO Fingerprint readers, PAC 512 access controllers must have their reader data jumper set to the 5V position.

It should be noted that Ievo readers cannot be used in conjunction with PAC readers on the same PAC512 controller.

3. Wiring Diagram for Revision 4 (IEVO_BOARD-R4)

The Revision 4 IEVO control board supports 2 IEVO readers (if required), with the additional reader being connected to Input B. The corresponding Output B may be connected to SIGB on the PAC 512 Controller for Read In/ Read Out, or to a separate PAC 512 door channel.



Power to the IEVO control board should be taken from the power supply of the PAC 512 access controller and protected by a suitably rated fuse: *IEVO Ultimate 800mA; IEVO Micro 630mA.*

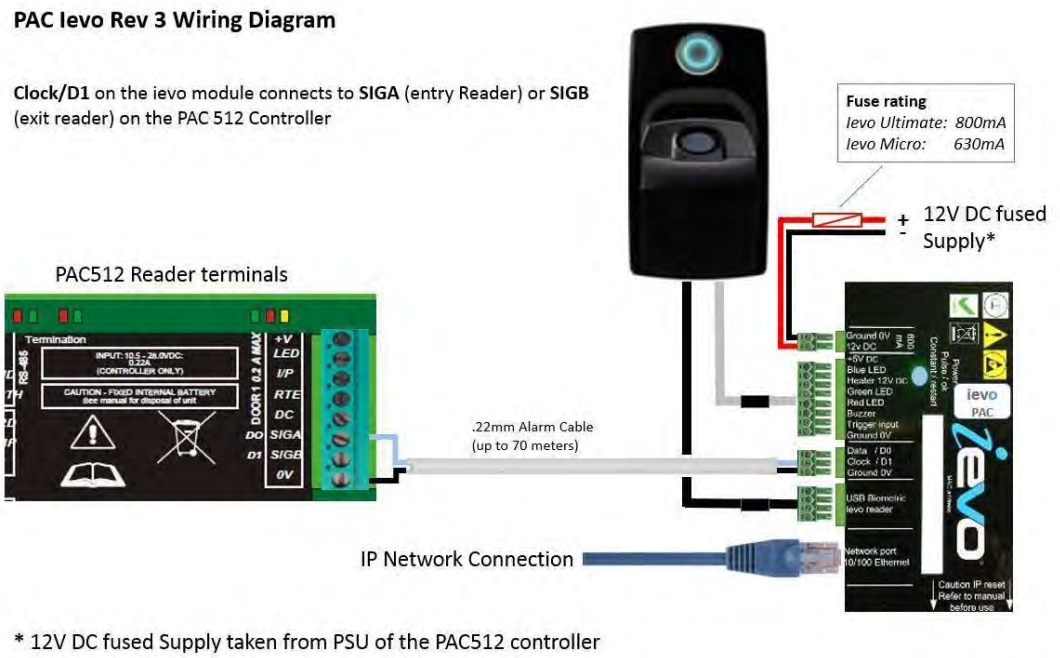
The IEVO control board connects to the PAC512 access controller using standard 0.22 mm alarm cable (up to a maximum of 70 Meters).

From IEVO control board	***To PAC512 access controller***
D0	SIGA (SIGB if used as an exit reader)
Ground	0V

The IEVO control board is connected to the Network via the Network In port (RJ45 Socket).

The Network Out port may be used to connect to an associated PAC 512IP access controller. Note, this connection must not be used as a network extension.

4. Wiring Diagram for Revision 3 (I_EVO_ACU)



Power to the IEVO control board should be taken from the power supply of the PAC 512 access controller and protected by a suitably rated fuse: *IEVO Ultimate 800mA; IEVO Micro 630mA.*

The IEVO fingerprint scanner is supplied pre-wired and connects directly to the IEVO control board as shown above.

The IEVO control board connects to the PAC512 access controller using standard 0.22 mm alarm cable (up to a maximum of 70 Meters).

From IEVO control board	*To PAC512 access controller*
Clock / D1	SIGA (SIGB if used as an exit reader)
Ground 0V	0V

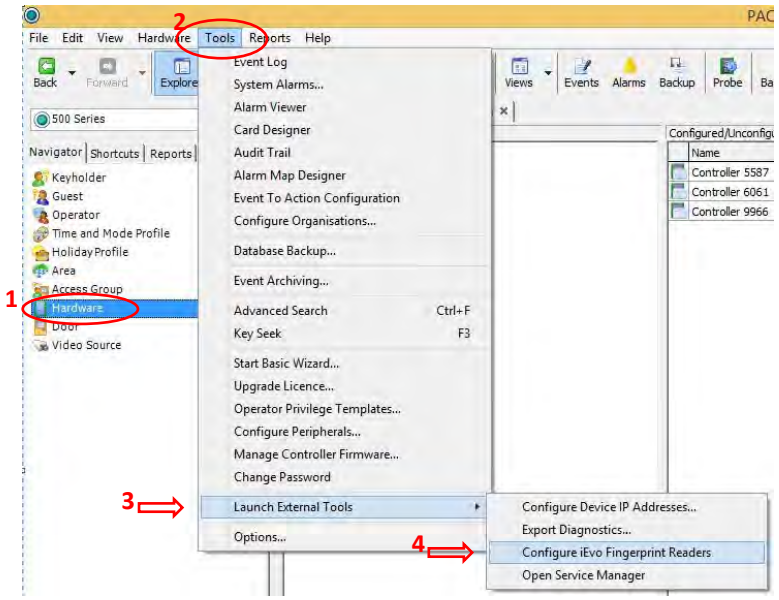
Note: *Data / D0 on the IEVO REV 3 control board is not used.*

The IEVO control board is connected to the Network via the Network port (RJ45 Socket).

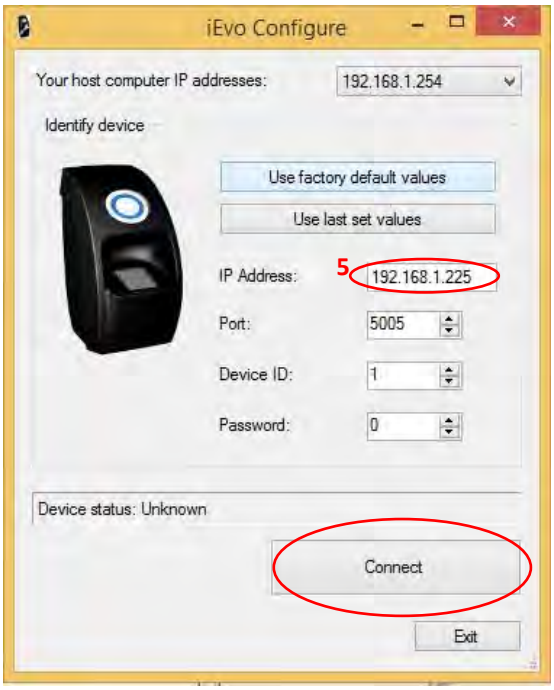
5. IEVO IP Configuration

Impotant Note: For configuration to proceed, the configuring PC must temporarily be set to the same IP range and subnet mask as the IEVO Control board. The default IP address of your IEVO board is 192.168.1.225 (Class C).

Follow the steps below to configure your IEVO for IP communication with PAC SecureNet using the relevant IP address, Subnet Mask, and Default Gateway for the host network.



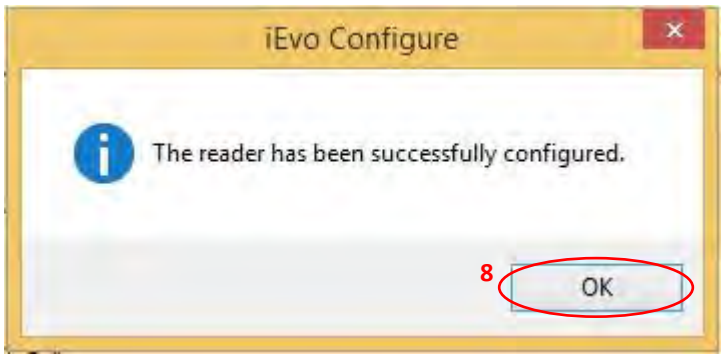
1. From the **Navigator** tab on the left of your screen, select the **Hardware** module.
2. Select the **Tools** menu from the SecureNet header.
3. Select **Launch External Tools**.
4. Select **Configure IEVO Fingerprint Readers**.



5. Enter the **IP Address** of the IEVO control board as shown above and click **Connect**. *Note: 192.168.1.225 is the default IP address of the IEVO control Board; this should be changed to an IP address that is compatible with the host Network.*

On connection to the IEVO control board, the following window is displayed. The IP address, Subnet mask and Gateway shown here are for illustration puposes only.

6. Enter the desired **IP Address**, **Subnet mask** and **Default Gateway** in the fields indicated above. Other settings must remain unchanged.
7. Click **Update reader.**



Upon successful configuration of the IEVO control board, the above message is displayed.

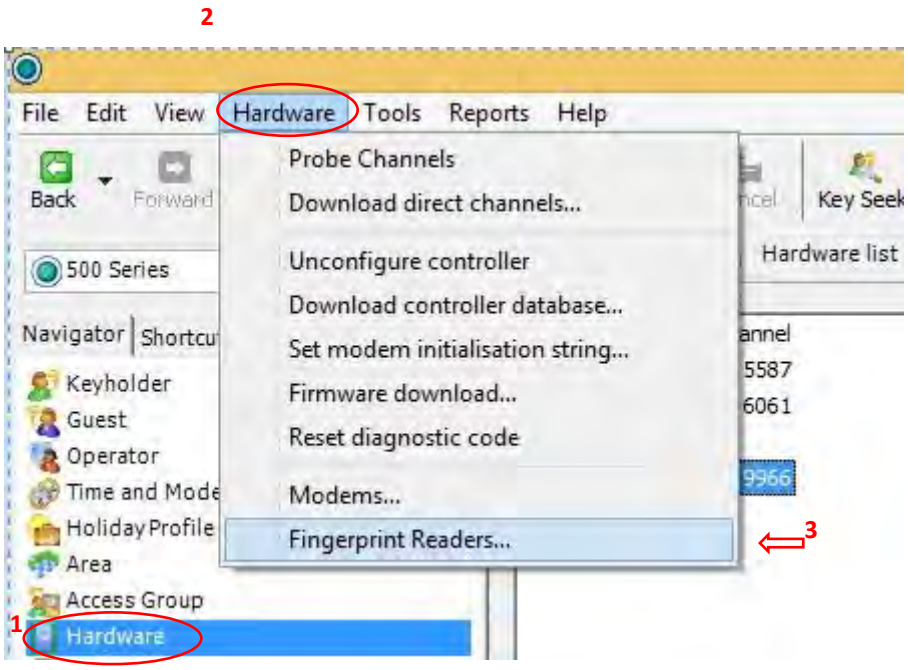
8. Click **OK** to complete IP setup.

9. Exit out of the 'Change reader configuration' and 'iEvo Configure' Screens, before proceeding to section 6 of this document 'IEVO door reader configuration'.

At this point, if there are no further IEVO devices to configure, the PC may be returned to its normal IP Address and Subnet Mask.

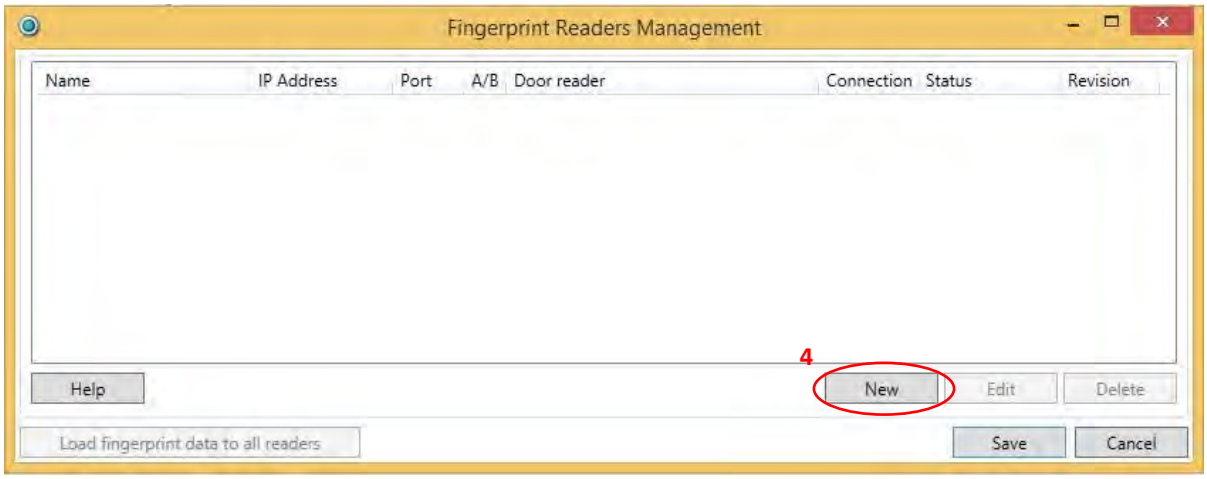
6. IEVO Door reader configuration

Follow the Steps below to configure your IEVO door readers within PAC SecureNet:

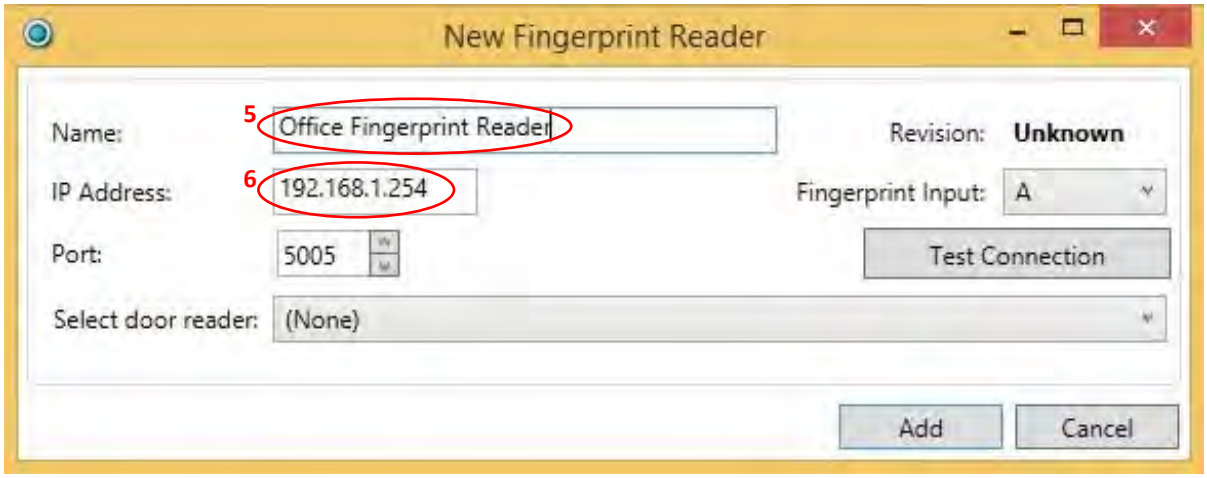


1. From the **Navigator** tab on the left of your screen, select the **Hardware** module.
2. Click **Hardware** in the header.
3. Select **Fingerprint Readers** from the drop down menu.

The Following Window is now displayed:



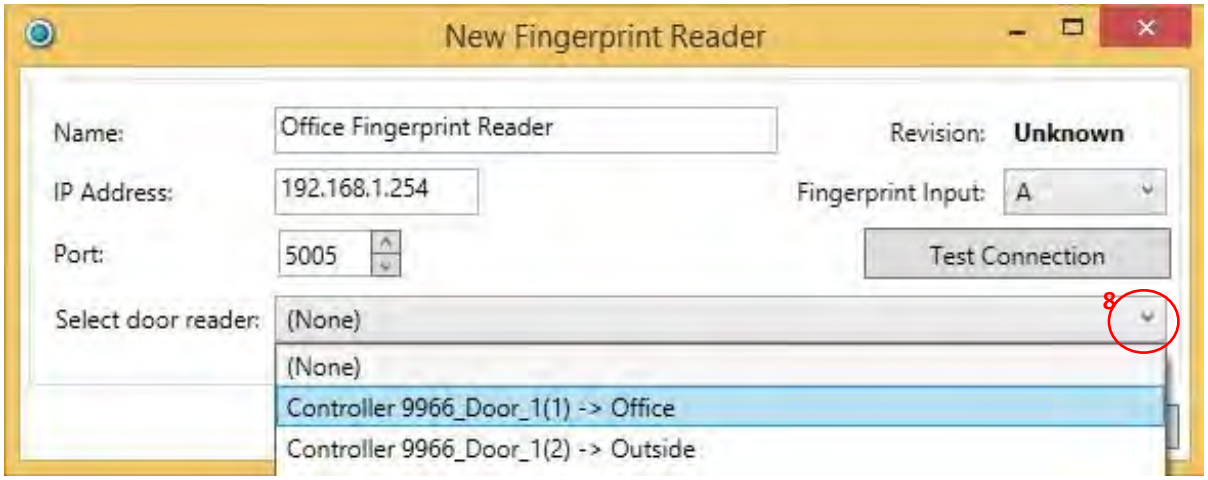
4. Click **New** to create a new IEVO Fingerprint Reader.



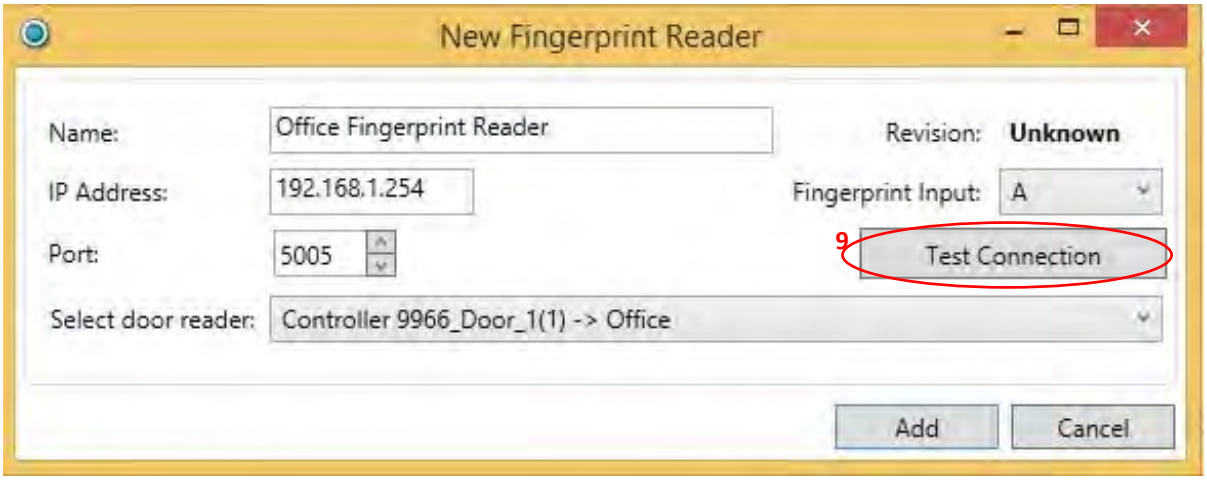
5. Input a **Name** for the new reader.
6. Input the **IP address** configured in Section 5 of this guide.

Note: The **Port** must remain unchanged at **5005**

7. Select the **Fingerprint Input** (**A** or **B**) that the reader is connected to on the IEVO control board.

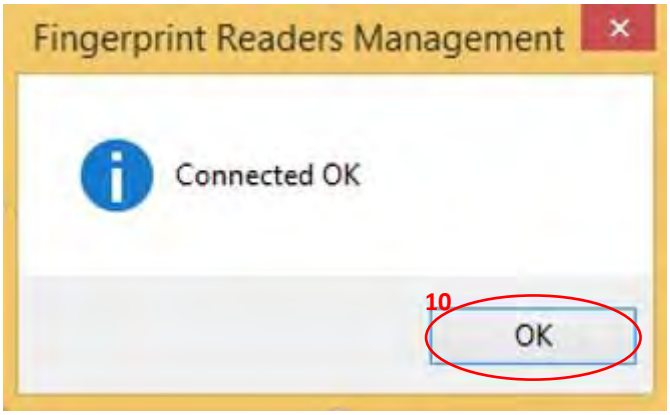


8. In the **Select door reader** section, use the drop down menu to select the Door that is to be controlled by the IEVO reader (Only Doors already created in PAC SecureNet will be displayed here).



9. Click **Test Connection** to test communication with the IEVO control board.

Successful communication is indicated as shown:



10. Click **OK** followed by **Add** to return to the **Fingerprint Readers Management** Screen.

If you have any further IEVO Control Boards to configure, proceed again from step 4 above.

11. Once all fingerprint readers have been configured, click '**Load fingerprint data to all readers'** to complete the configuration process.

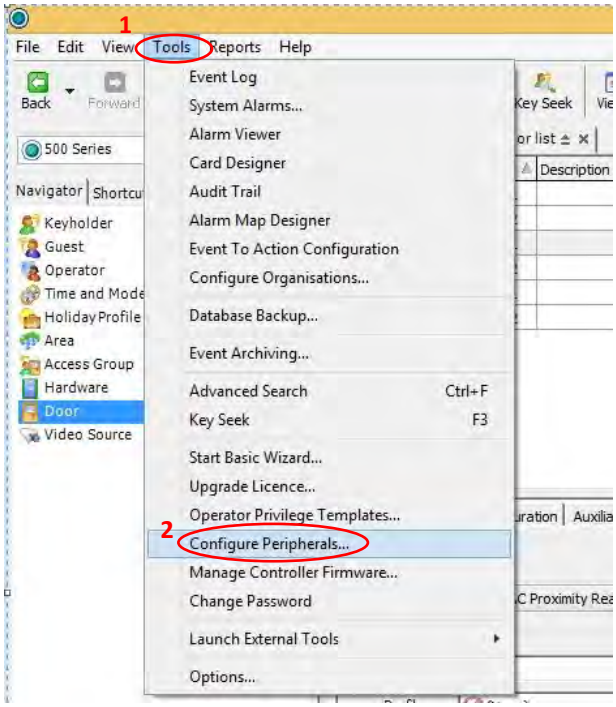
12. Click **Save** to store your reader configuration.

7. IEVO Administration reader configuration

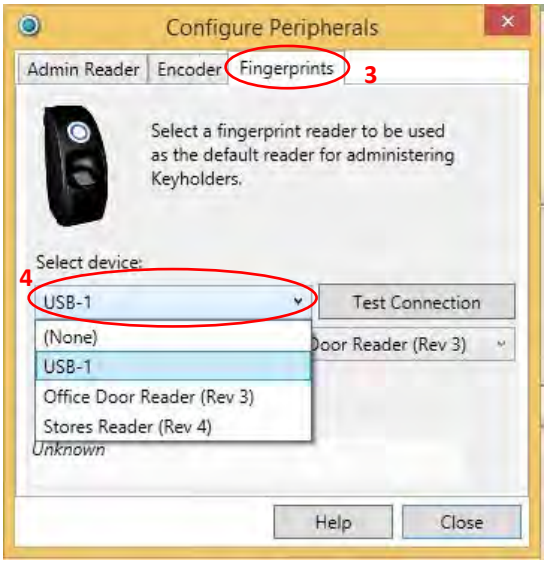
If an IEVO USB Desktop enrolment reader is to be used, ensure the USB driver is installed before proceeding. The correct driver can be found on the disc provided with your enrolment reader.

Drivers may also be found within your PAC SecureNet Disc/Download in the following location: USB\IEVO USB Admin Kit\USB desktop drivers.

Follow the Steps bellow to configure your IEVO administration reader.



1. Select the **Tools** menu from the SecureNet header.
2. Select **Configure Peripherals** from the drop down menu.

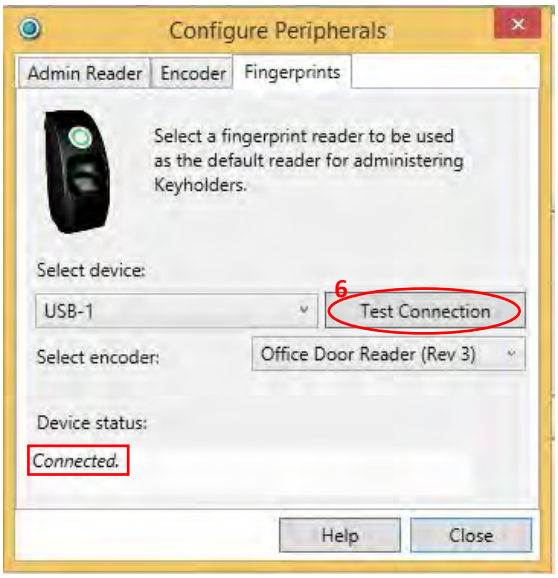


3. Select the **Fingerprints** tab.

4. Select the Device that is to be used for Fingerprint enrolment; this may be either a USB desktop reader (USB-1) or any Door reader. Selection of a door reader for fingerprint enrolment does not affect the readers' normal operation.

5. From the **Select encoder** drop down list, select the Device that is to be used as the encoder; this can be any connected IEVO control board. This selection does not affect the normal operation of the control board. Any connected reader will however become 'busy' for 1 or 2 seconds during the actual enrolment process.

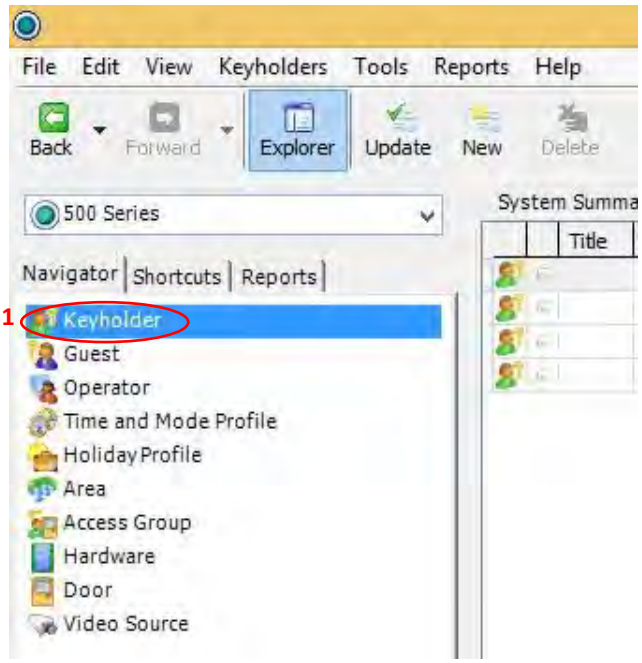
   Note: *The designated encoder assumes the role of converting fingerprint scans into usable biometric data.*



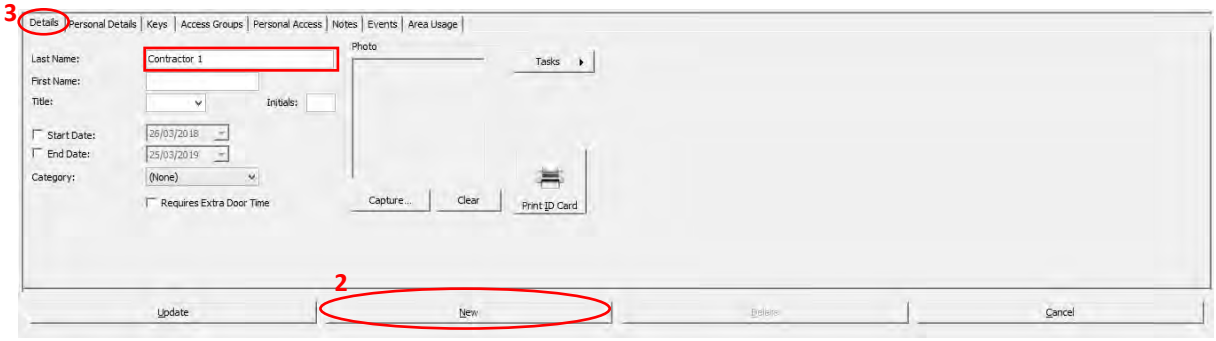
6. Click **Test Connection** to confirm communication with the selected devices. On completion of a successful test, the **Device status** field will display '***Connected'.*** The 'Configure Peripherals' window may now be closed.

   This completes administration reader configuration.

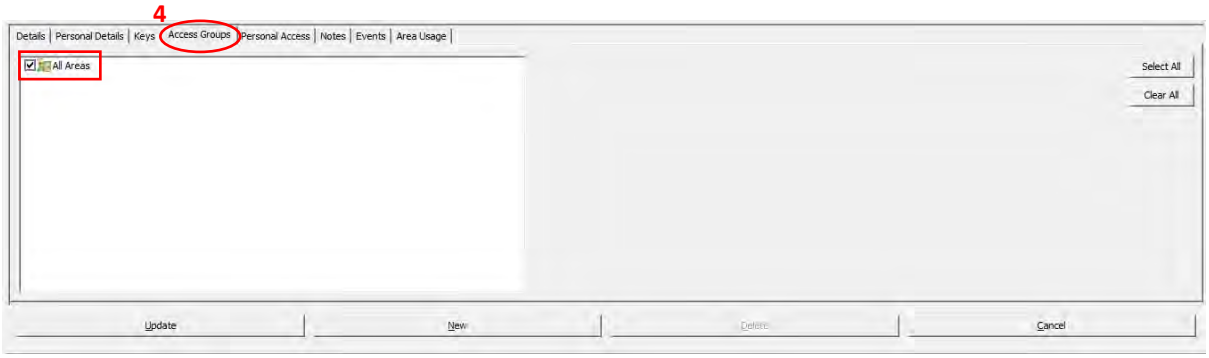
8. Fingerprint Enrolment



1. From the **Navigator** tab on the left of your screen, select **Keyholder**.

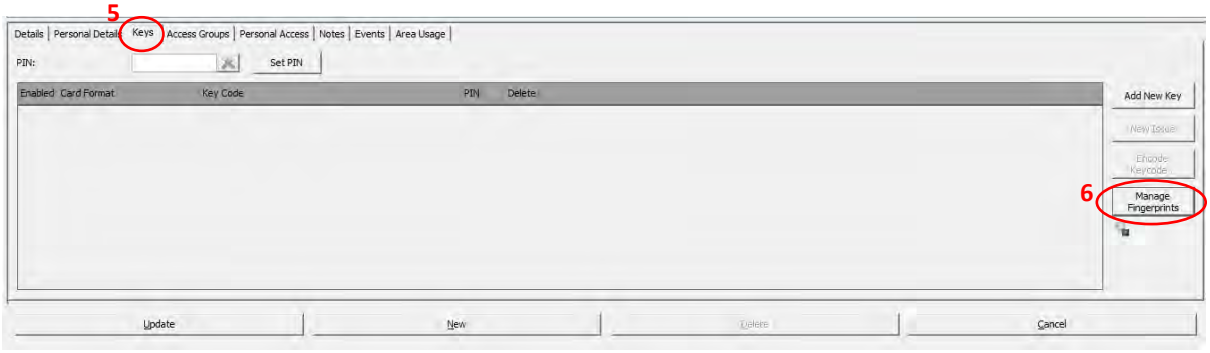


2. At the bottom of the screen, click **New** to begin enrolling a new Keyholder.
3. In the **Details** tab Input the Key holders **Last name** (mandatory field) and any further information as may be required.

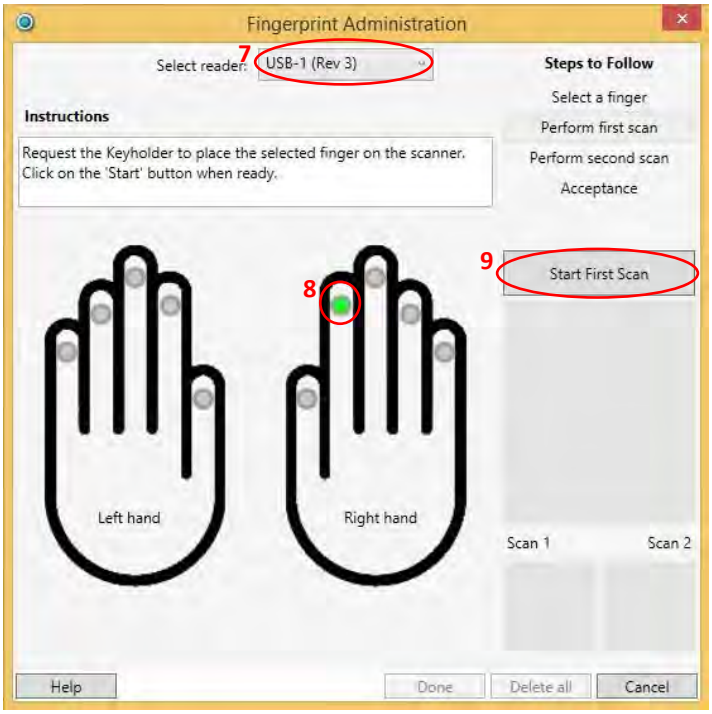


4. Click on the **Access Groups** tab and select an access group appropriate to the key holder.

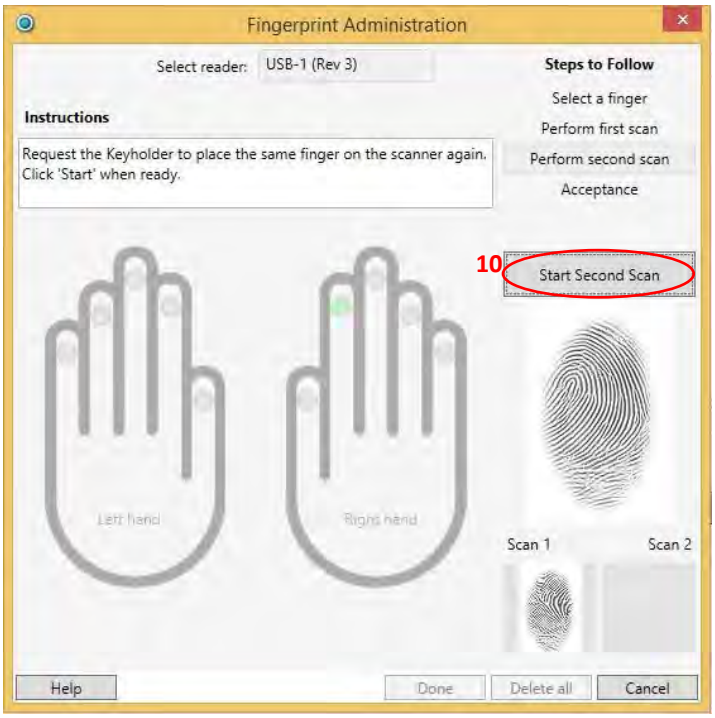
5. Click on the **Keys** tab.



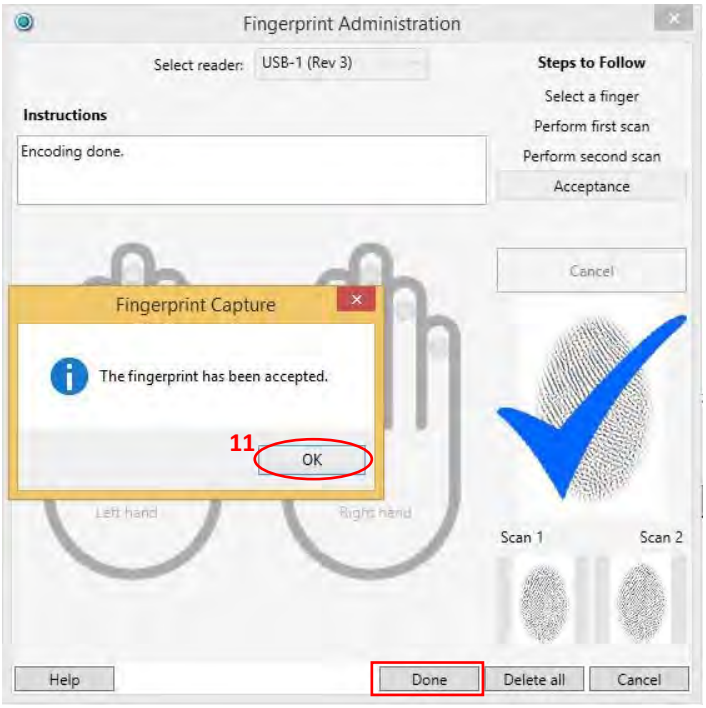
6. Click **Manage Fingerprints** to begin fingerprint enrolment.



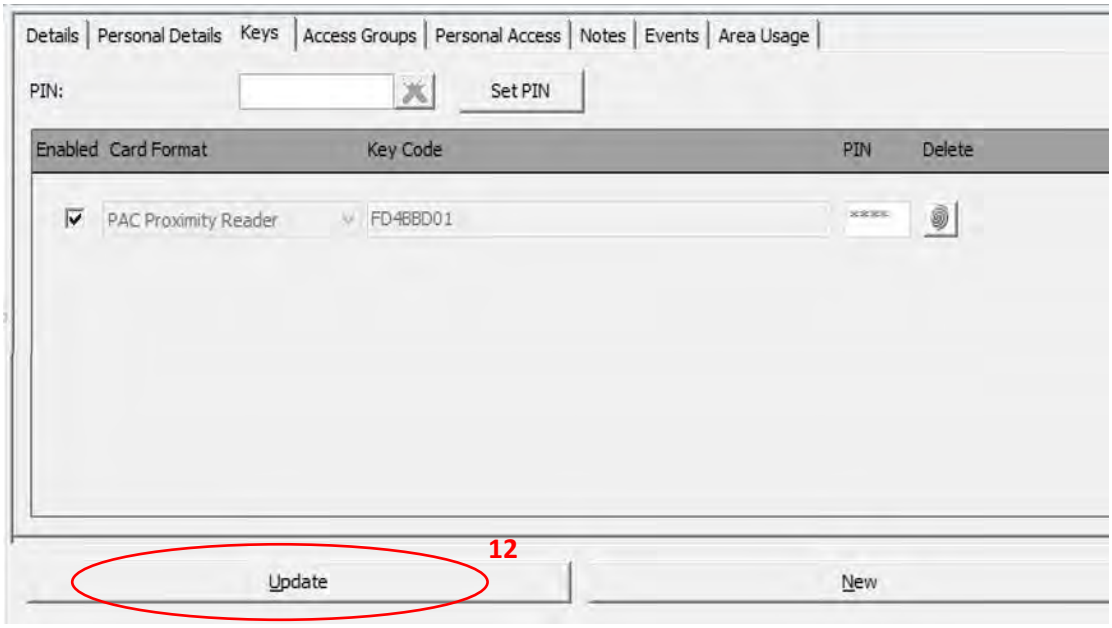
7. Select your chosen administration reader from the **Select reader** drop down list.
8. Choose the finger you wish to enrol by clicking the corresponding circle.
9. Have the Key holder place their finger on the scanner and click **Start First Scan**.



10. When indicated, as shown above, have the Key holder lift and replace their finger on the scanner before clicking **Start Second Scan**.



11. Upon successful fingerprint capture, click **OK** to proceed. Any additional fingerprints may now be captured as previously described. When all desired fingerprints have been captured, click '**Done'**.



12. Click **Update** to store the captured fingerprints to the database.

Keyholders with enrolled fingerprints will display the fingerprint icon in their Keys list, as shown above.

As more fingerprints are enrolled, they will automatically be loaded to all relevant IEVO readers; the associated Key Codes will automatically be loaded to the corresponding PAC512 controllers.

Fingerprints may be reloaded to all readers at any time by clicking 'Load Fingerprint Data to all readers' as shown in section 6 – 12 of this document.

This concludes configuration of for your PAC IEVO hardware.

Appendices:

Appendix A: Revision 4 Control Board IP Reset

Press and Hold the reset button (SW1) on the IEVO control Board for 10 Seconds

Appendix B: Revision 3 Control Board IP Reset

1. Remove all connections from the IEVO board
2. Hold down the Reset switch
3. Connect power, wait 10 seconds, then down power
4. Release the reset switch

Appendix C: Default settings after reset:

ID: 1

IP: 192.168.1.225

Password: 0

Port: 5005