ScreenCheck

BADGEMAKER 7

SC Biometrics

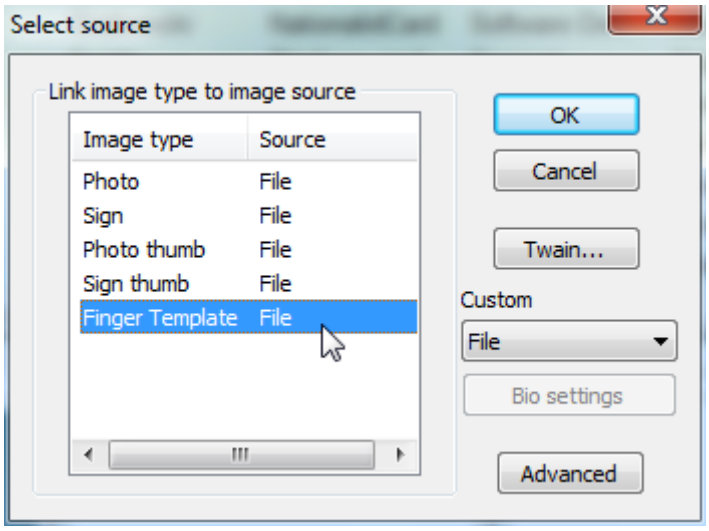
· ID DESIGN · MANAGE · PRINT SYSTEM ·

www.screencheck.com

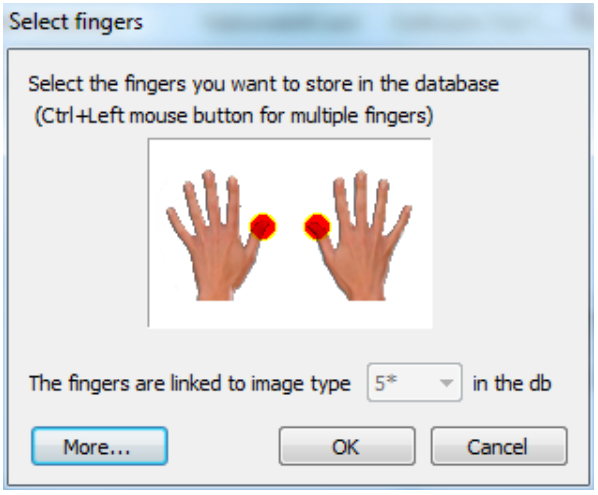
SCREEN CHECK

1. Select Source for SC Biometrics

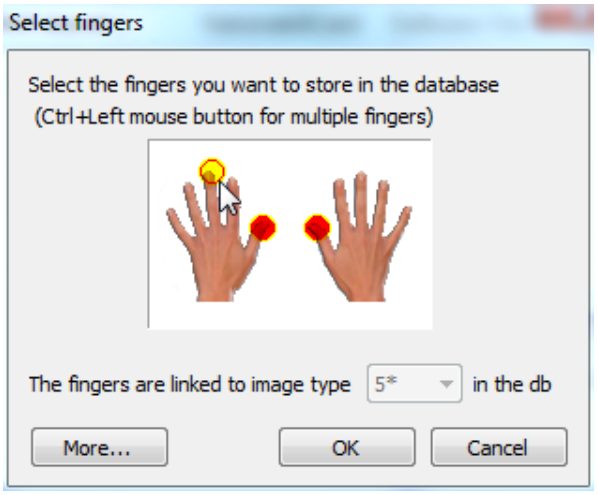
Choose **Select Source** from the **Image Menu**. Select the desired image type to link to the **SC Biometric image source**. Select **SC Biometrics** from the **Custom** dropdown list.



Select source Click the **Bio Settings** button to modify device settings.



Select Fingers Use **Ctrl+Left** mouse button to select multiple fingers to scan.



Select multiple fingers , click **More**, the following dialog box is presented.

- **These settings are only configured in combination with NEC enabled devices.**

1.1.1 Scanner

Select your device model from the drop down list.

1.1.2 Security

Select the level of security. Low security will allow easy and quick scanning but there is a chance different fingers will give a positive match. If you select the maximum security the verification is more secure but sometimes it is difficult to enroll all fingers. It is best to start with a high level of security, in the case the finger enrollment causes errors you can step down a level on security.

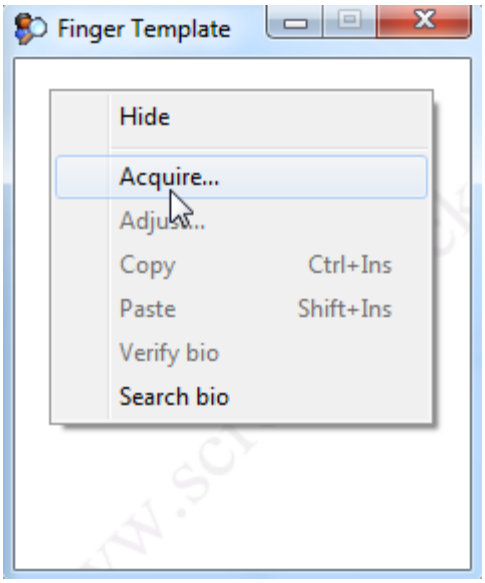
1.1.3 Scans

ScreenCheck advise to make at least two scans. If you do only one scan, there is a good chance that a finger is unsuccessfully enrolled.

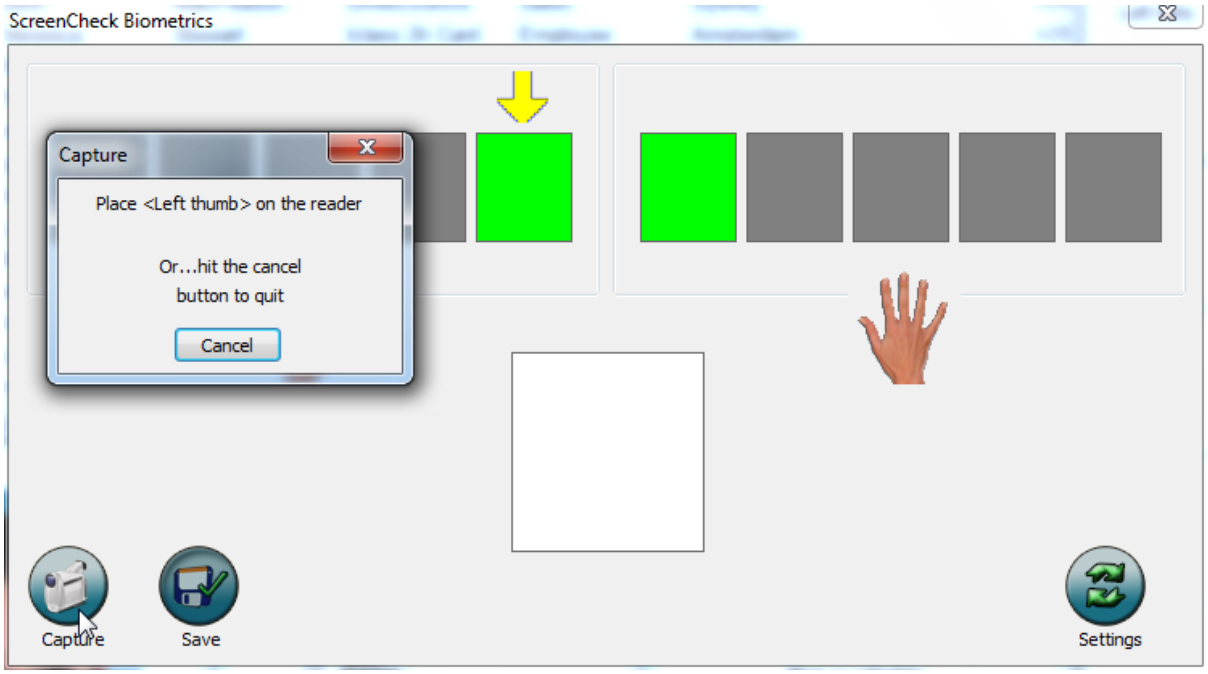
You can scan up to **10** fingers. To select multiple fingers hold down the <CTRL> button whilst clicking with the left mouse button on a finger.

2. Acquire SC Biometrics

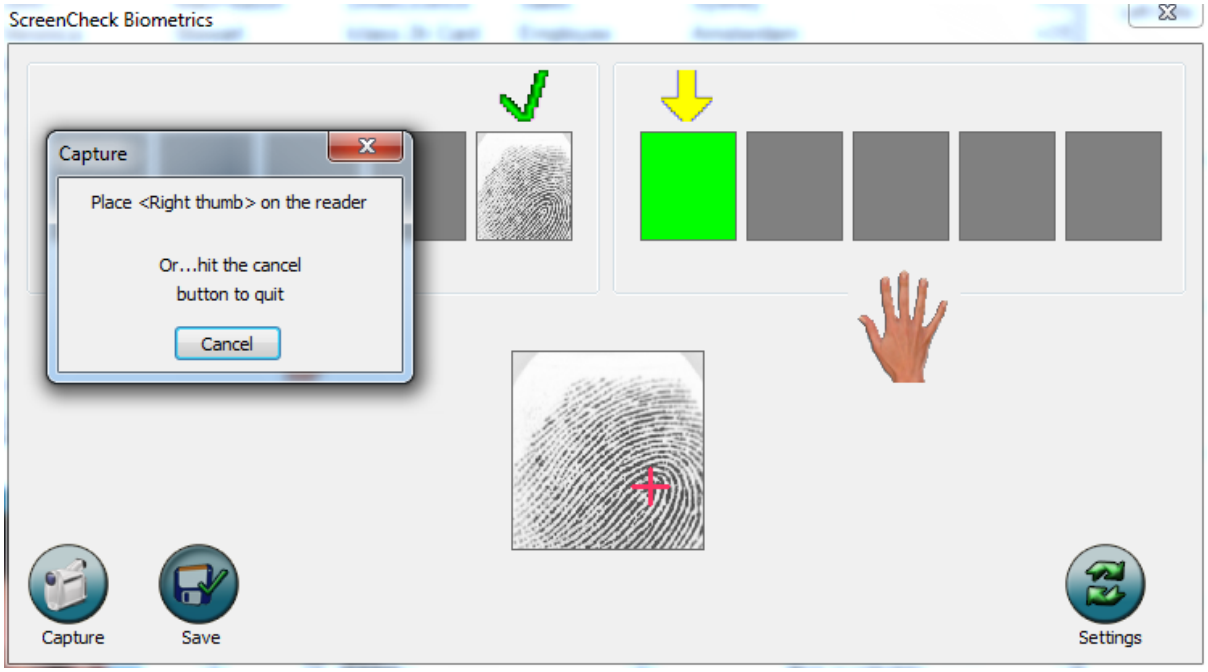
Select the correct image type such as the "*Finger Template*" window for example, and right click with your mouse then click **Acquire**.



The SC Biometric Plug-in will initialize. After a short communication with the scanner, the **SC Biometrics** window will appear. Click **Capture** to begin scanning.



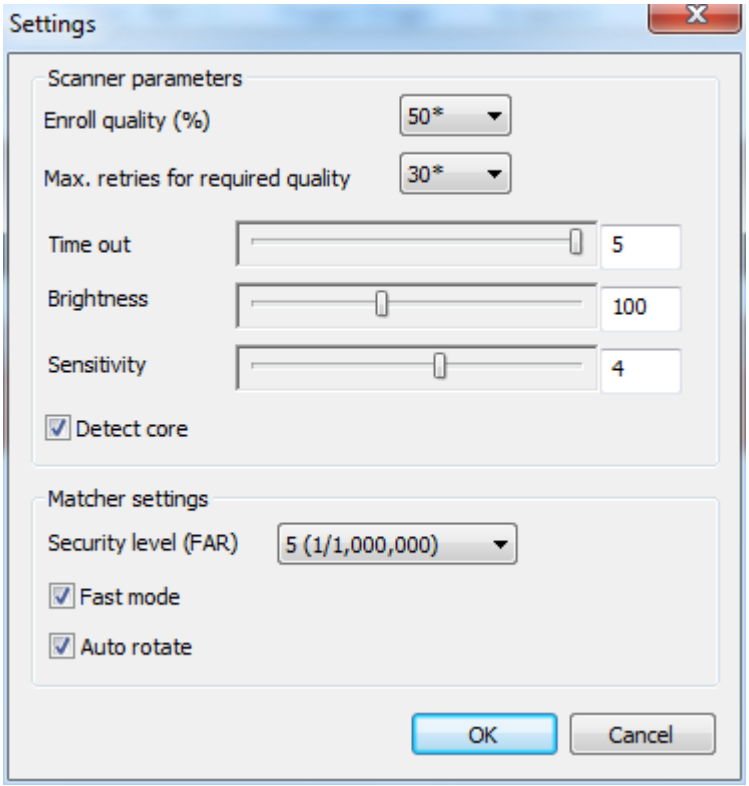
Follow the instructions on the screen carefully and scan all required fingers indicated by the color **GREEN**. Place your finger on the scanner to acquire and image, the plug-in will capture a scan once the finger has been recognized by the reader.



When a finger is scanned successfully it will be displayed with a green checkmark above it. The **red** marker above will indicate a failure to read your finger and should be scanned again. Each finger scan is displayed separately.

2.1 Settings

Click Settings to configure the following:



2.1.1 Scanner parameters Time out: Set the amount of seconds per session needed to capture. Once the time limit has been reached the session is disconnected. **Brightness:** Set the brightness for your images. Higher value means darker image. Default value is 100. **Sensitivity:** Set the sensitivity for the sensor on the reader. Value ranges from 0 to 7. A higher value means more sensitivity. Default value is 4.

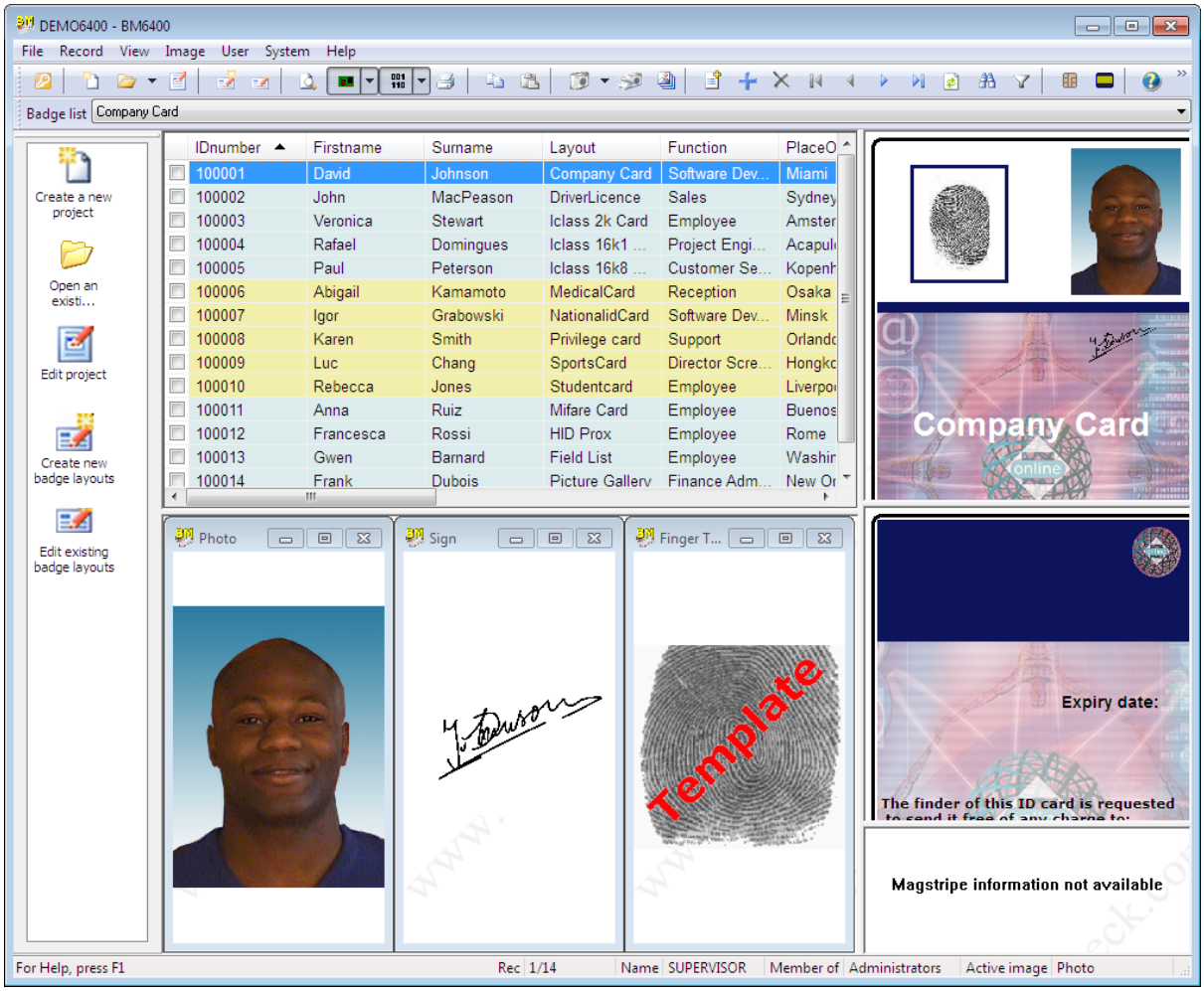
Detect Core: When enabled the reader will locate a unique reference point on the finger usually located in the central area of the fingerprint. By Default this feature is enabled.

- **This setting should be enabled to obtain more accurate fingerprints – the verification may fail if the image captured is not good enough. Enabling Detect Core ensures a more accurate fingerprint.**

2.1.2 Matcher settings Security level (FAR): Set the level of security, this ranges from 1 to 7 being the most secure verification. FAR (False Acceptance Ratio) Refers to the percentage of acceptance by unregistered fingerprints .

Fast mode: Set the speed in which identification takes place. **Auto rotate:** Rotate the template of a fingerprint enrolled 180 degrees.

Select **Save** to transfer the scanned fingers to the database. The images and templates of captured fingers will be stored in one BLOB (*Binary Large Object*).



Finger images can then be displayed on a badge. Finger images and templates can be stored in **2D Barcode**, in a **contact chip** or in a **Mifare chip**.

- **Please note that the finger images in general are too big to store in a barcode or Mifare chip and is not commonly done unless requirements insist.**

After saving the biometrics data, you can begin finger verification to **Verify Biometrics**.

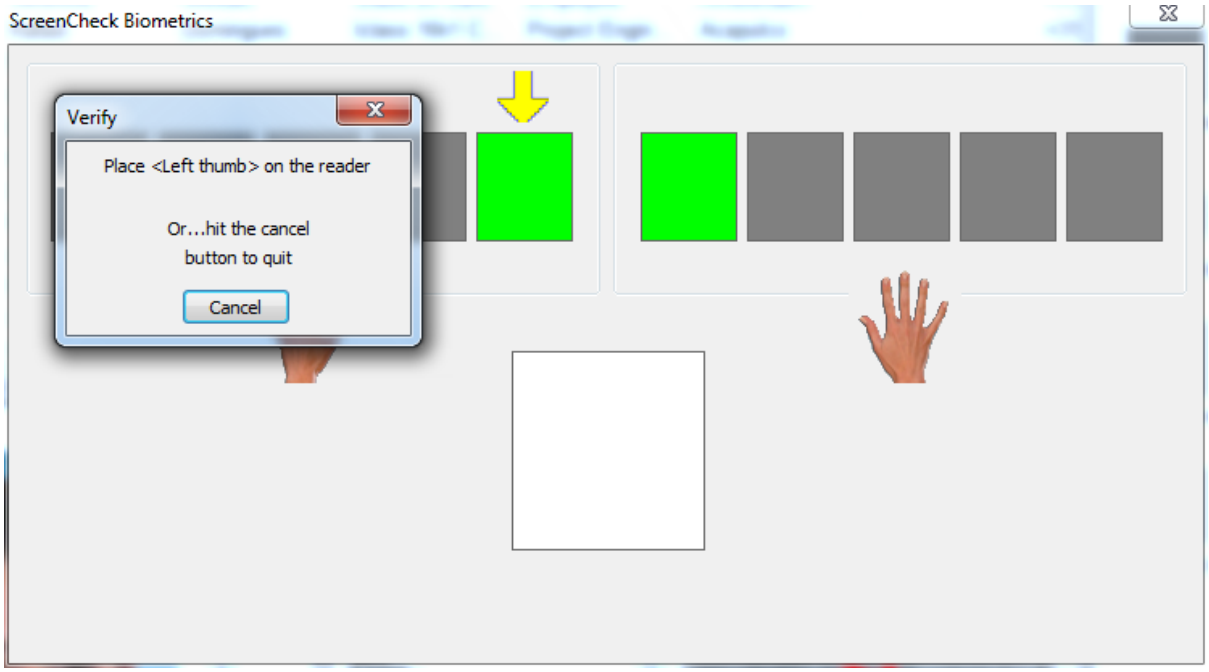
.

3. Verify Bio

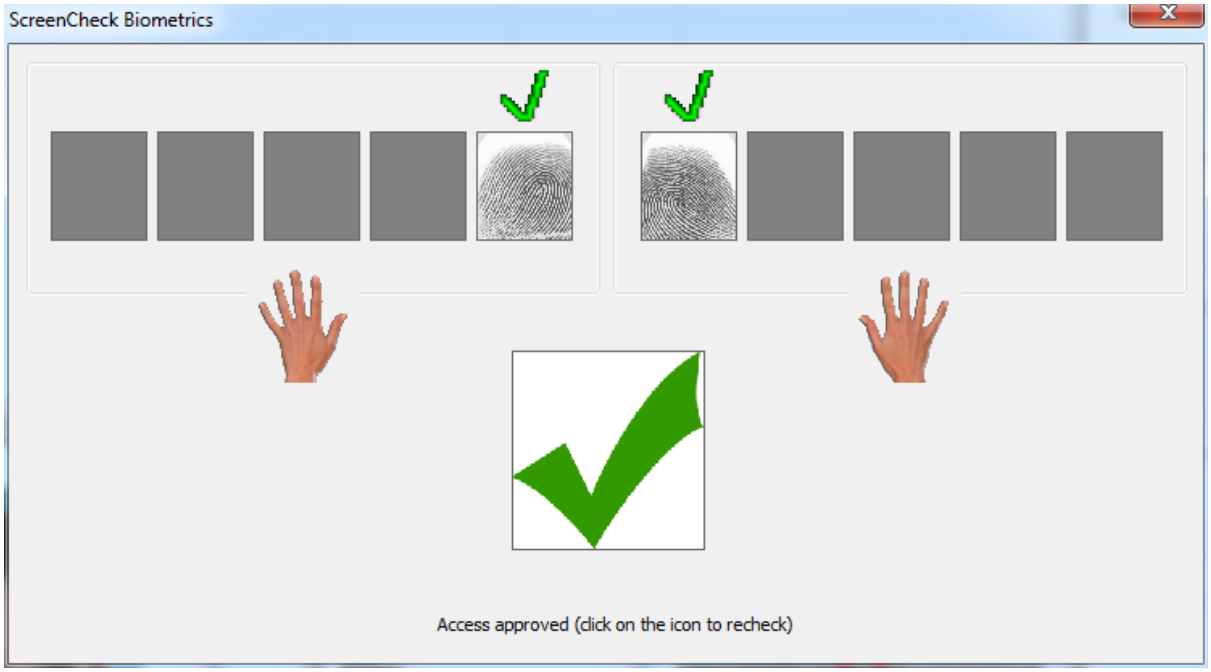
The option **Verify Bio** is only available when **SC Biometrics** has been installed, if SC Biometrics is not installed than **Verify Bio** will remain disabled.

SC Biometrics can carry out verification matching a current taken scan with the saved characteristics of a scan in the database. This is useful to identify an existing person in the database or to verify scan is operating successfully.

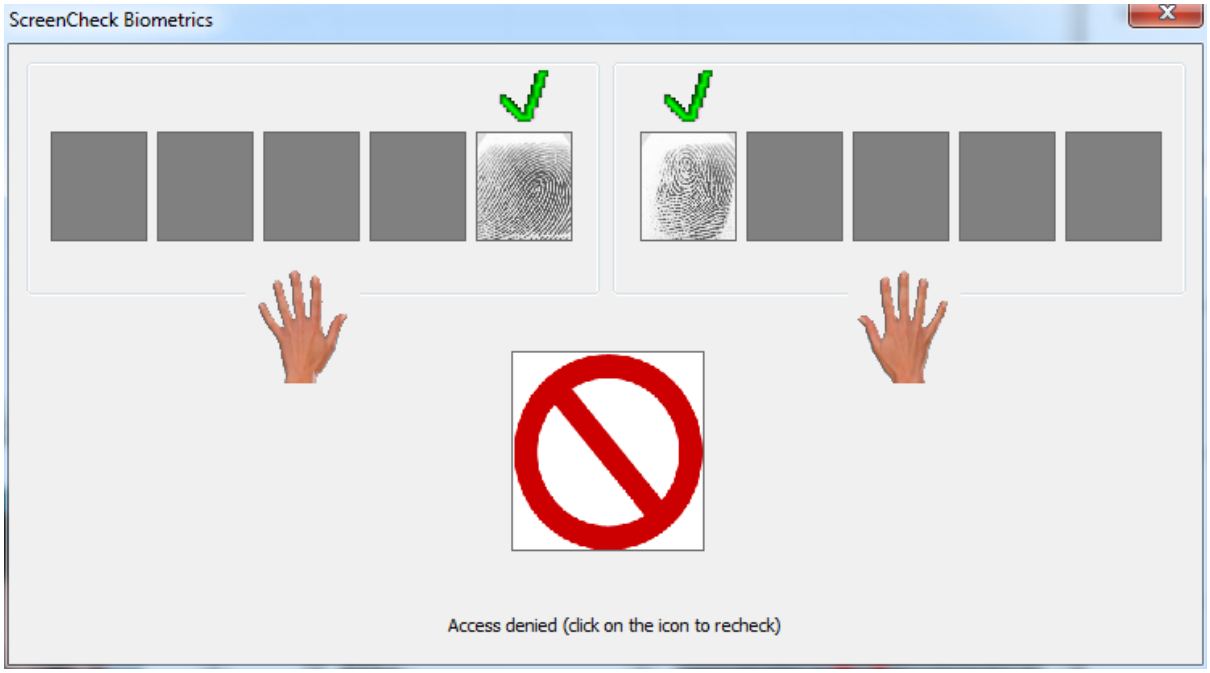
To begin a search, please select the **Image Menu** and then select **Verify Bio**.



Present the indicated finger and lay it onto the surface of the scanner. The finger is scanned and matched to the current selected image in the database. If the verification was successful you will see the following dialog.



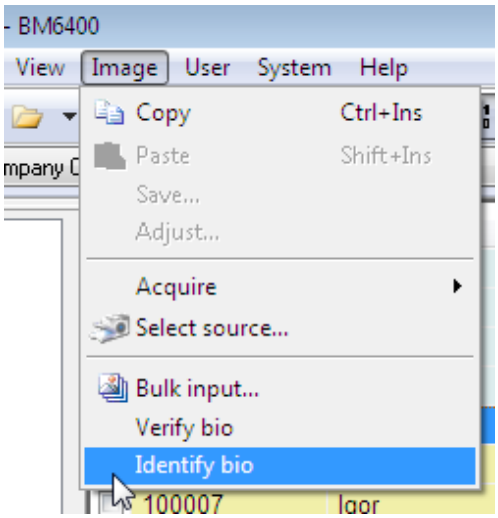
If the verification process is unsuccessful you will see the following dialog



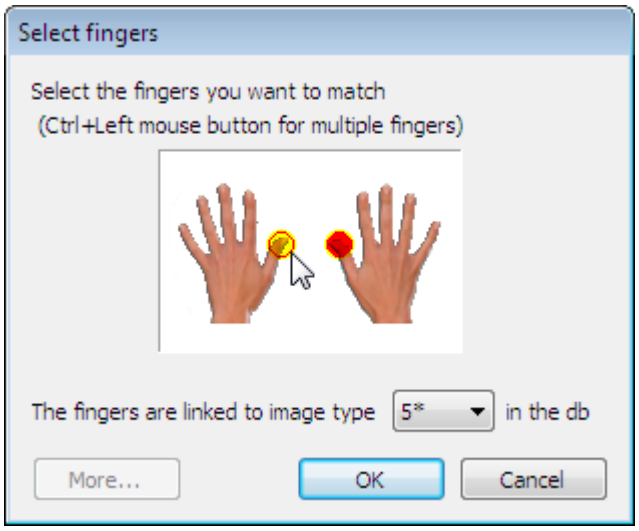
SC Biometrics **Verify** does not acquire an image. You must select **Acquire** to obtain an image. If multiple scans have been captured and you select **Verify Bio**, the same procedure is carried out but multiple verifications will take place.

4. Identify Bio

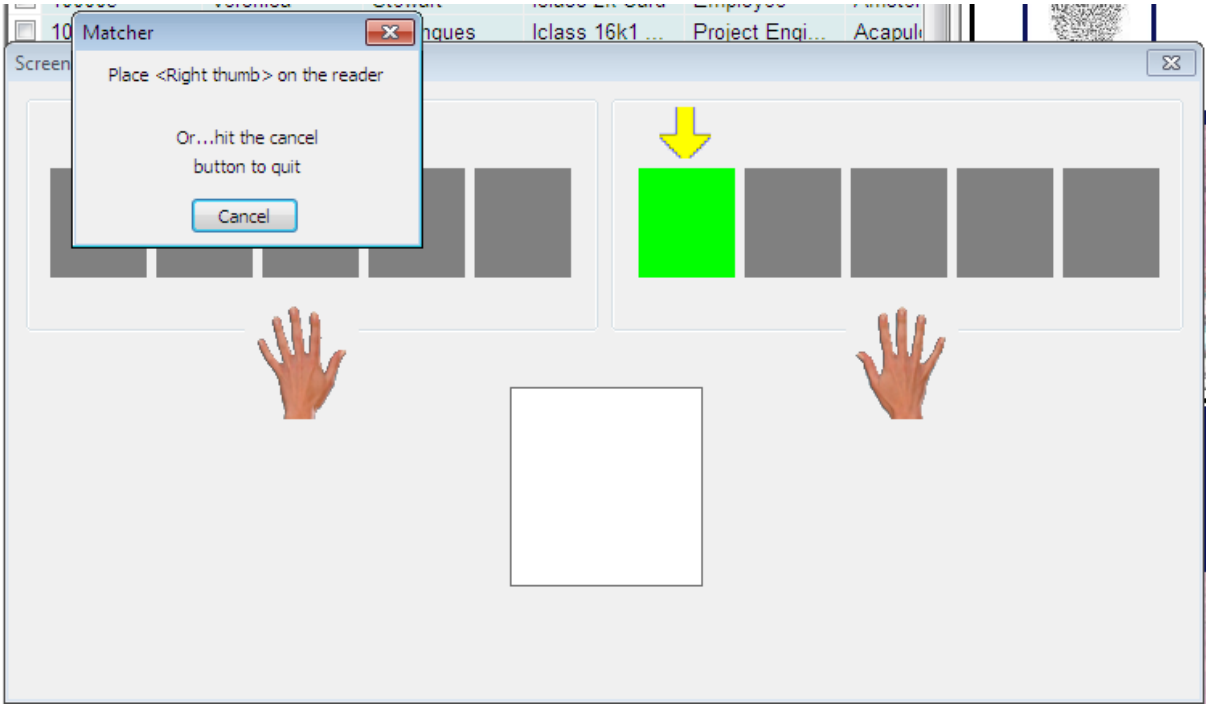
To access select **Identify Bio** from the **Image Menu** or right click inside the Finger Template window with the right mouse button and select Identify Bio.



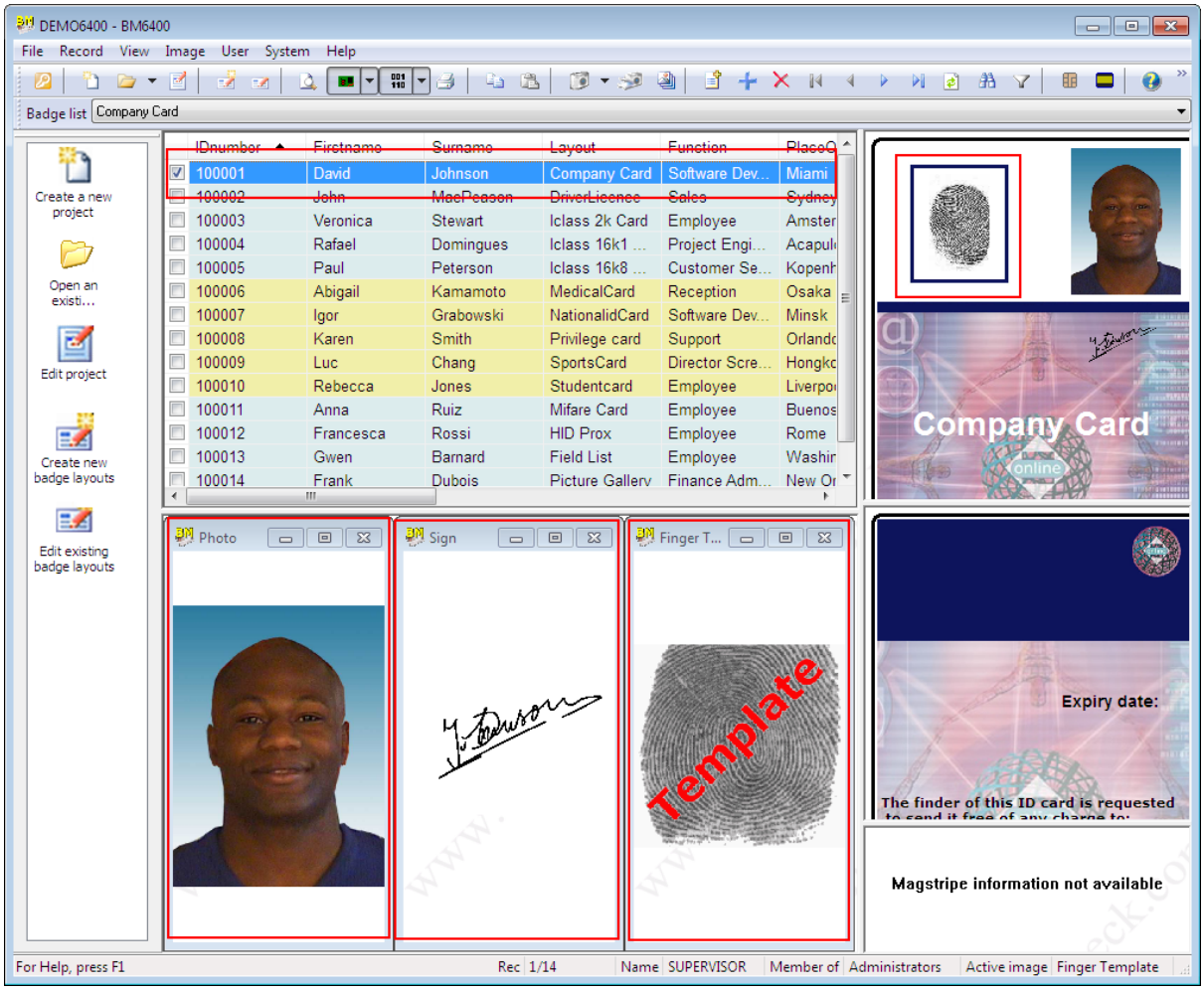
Select this feature to search the database for an individual record based upon his/her fingerprint.



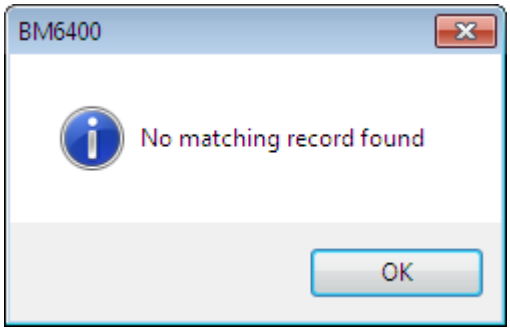
Click **Ok**.



Present the indicated finger and lay it onto the surface of the scanner. The finger is scanned and matched to an existing fingerprint already tied to a record in the database. If the verification was successful you will see the record tagged in BadgeMaker.



If the identification process was unsuccessful and no existing record is identified the following dialog is presented.



- **This feature is only available if Fingerprint templates already exist in the database. The Finger Template window must be active in order to select Identify Bio from the Image Menu.**