	Sensor Integration

Contents

Introduction

GuardPoint Pro since version 2.03.0xx supports selected SENSOR biometric readers. The integration allows enrolling fingers from any one of the readers and automatically downloading the finger templates to all the readers within the cardholder's access group.

Supported readers

Three models of Sensor fingerprint readers: SensorBio. Each of them may support either EM-Marine cards or 13.56MHz Mifare 1K Cards. The relevant models are as follows:

SensorBio: EM: S-BIO-KP, Mifare: S-BIO-KP-M

SensorBio :EM: S-BIO-SP, Mifare: S-BIO-MF

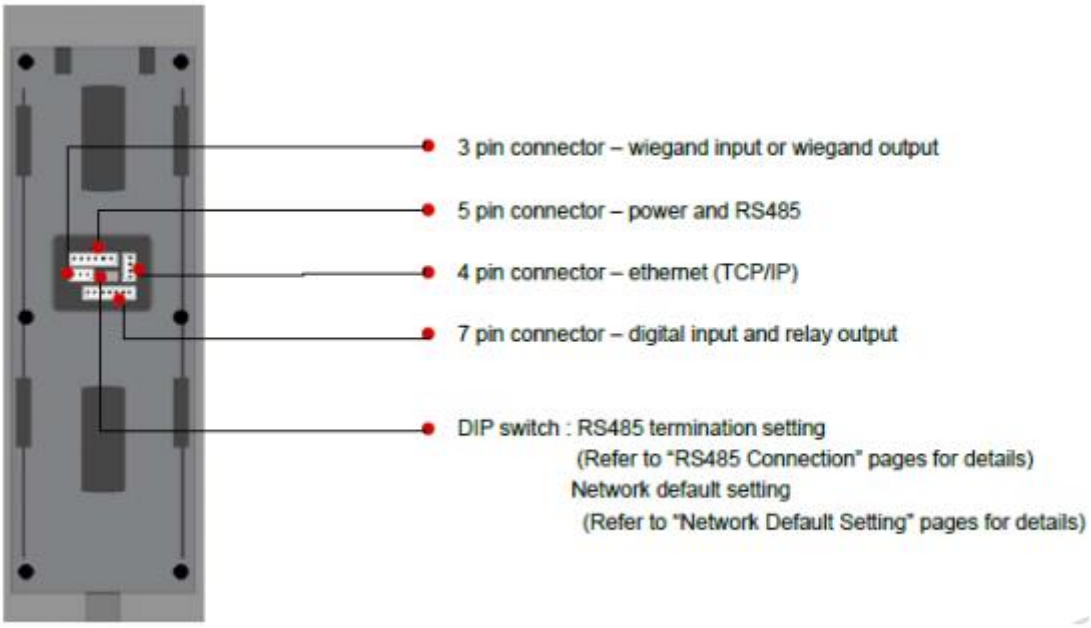
SensorBio :Mifare: S-BIO-MF-W,

In addition, the **Sensor Bio USB**, the USB enrolment reader of Sensor is supported.

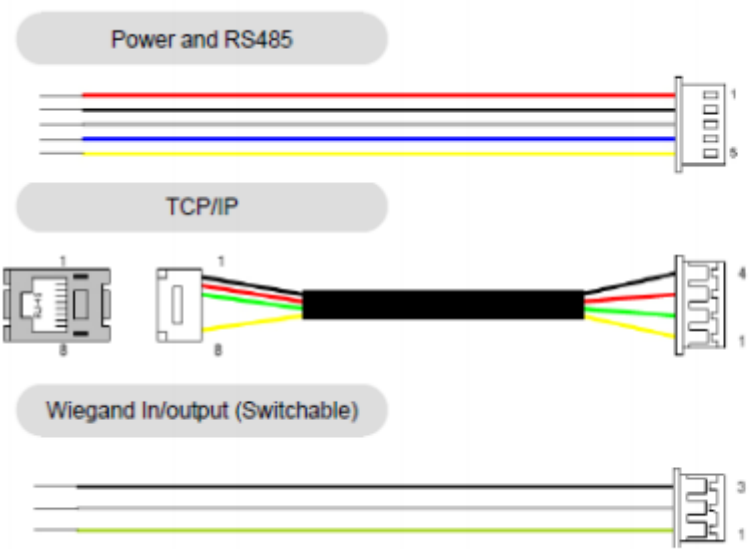
Connection

Note: The connection details re the reader connection in this document were copied from Sensor technical manual and appear here only as easy reference tools. For full & updated data consult the relevant Sensor manuals & datasheets. Sensor web site: http://www.sensoraccess.co.uk

The rear side of the Sensor**Bio** reader has four sockets for cables and one DIP-Switch.



The cables that are relevant for the integration are three:



PIN	PIN DESCRIPTION	WIRE
1	POWER +12V	RED
2	POWER GND	BLACK
3	RS -485 GND	GRAY
4	RS -485 TRX+	BLUE
5	RS -485 TRX-	YELLOW

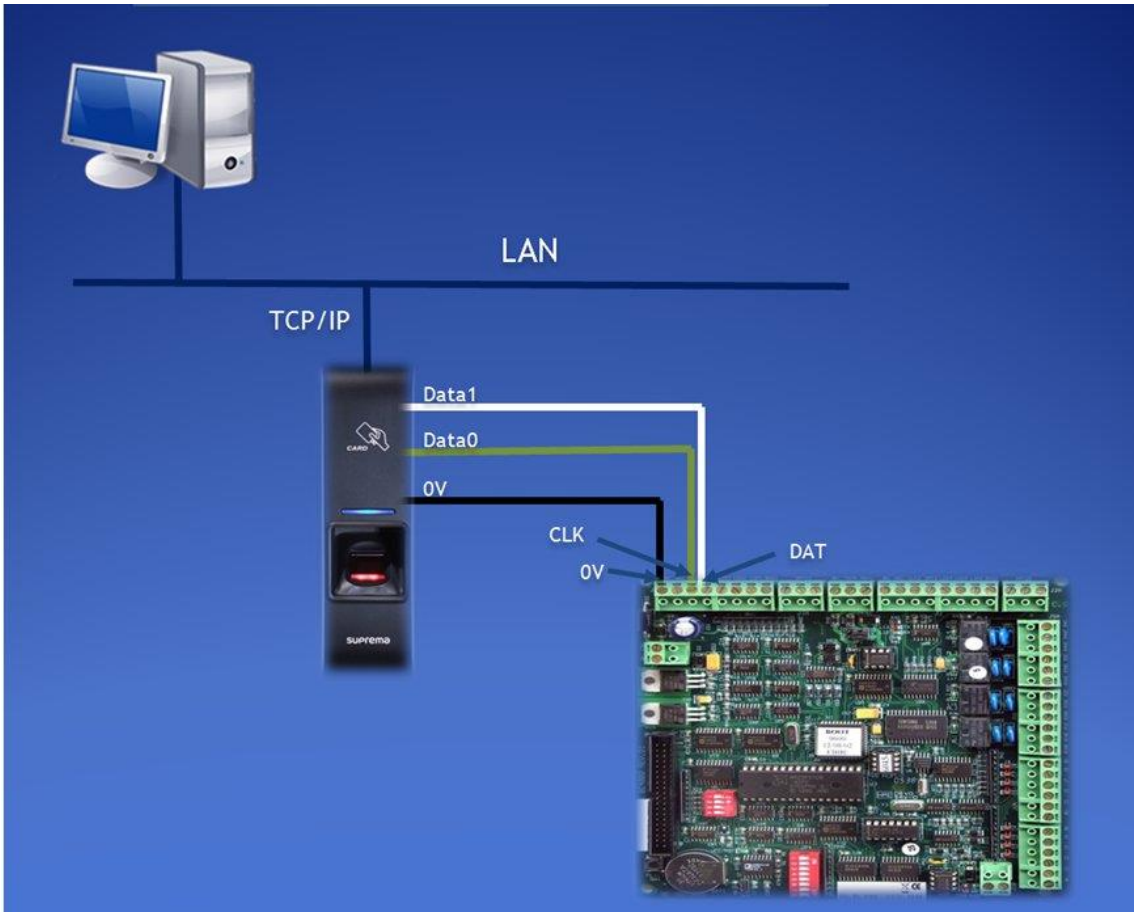
PIN	PIN DESCRIPTION	WIRE	RJ45 PIN
1	TX +	YELLOW	6
2	TX -	GREEN	3
3	RX +	RED	2
4	RX -	BLACK	1

PIN	PIN DESCRIPTION	WIRE
1	WIEGAND DATA0	GREEN
2	WIEGAND DATA1	WHITE
3	WIEGAND GND	BLACK

The reader should have two connections simultaneously:

1. **Communication** (to receive configuration and templates)**.** Communication to PC, by RS485 or TCP/IP. (In case of RS485 consult Sensor technical documentation to know how many readers can share the same RS485 bus).

2. **Wiegand** (to send the cardholders' code)**.** Wiegand-Out to Sensor Controller Reader input connector.



BioStar

The BioStar is the Sensor utility software. As far as the GuardPoint Pro integration is concerned the BioStar is needed for the following uses:

1. For the initial identifying of the unit via RS485. This step is a must even if later the reader is supposed to communicate via TCP/IP.

2. For setting the reader's IP address

Note: This manual assumes that you have successfully installed BioStar and that the Sensor readers are already setup as 'Devices' on BioStar with good communication. For any issues relating the installation and setup of BioStar please refer to the relevant Sensor documentation.

Defining the Sensor reader in GuardPoint Pro

a. Open the main GuardPointPro.INI and set

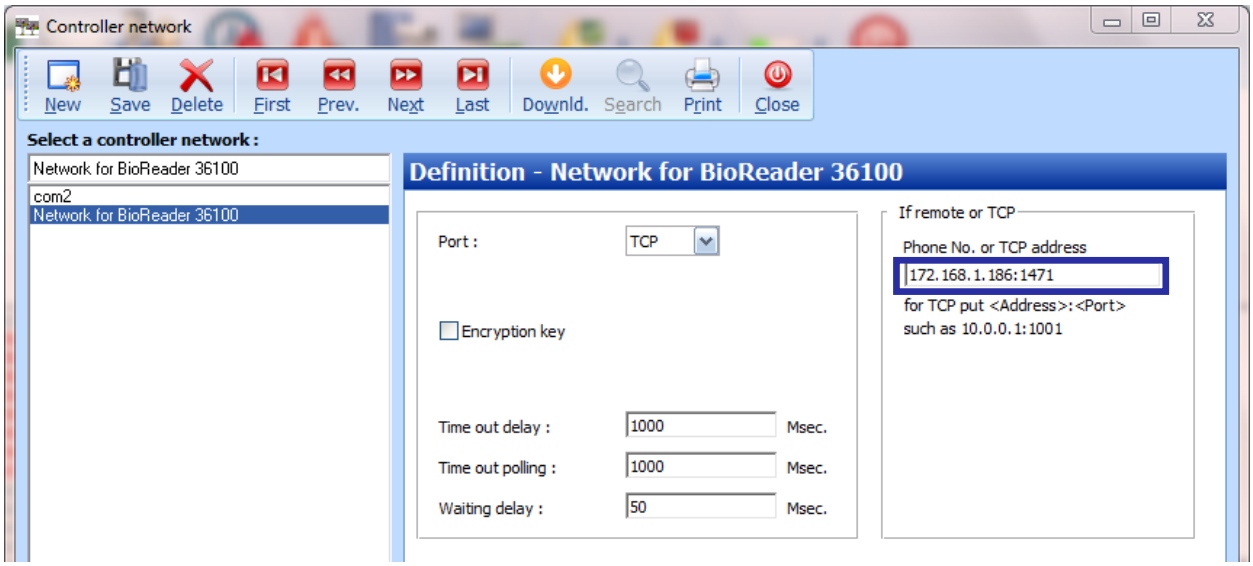
Sensor= 1

Restart GuardPoint Pro .

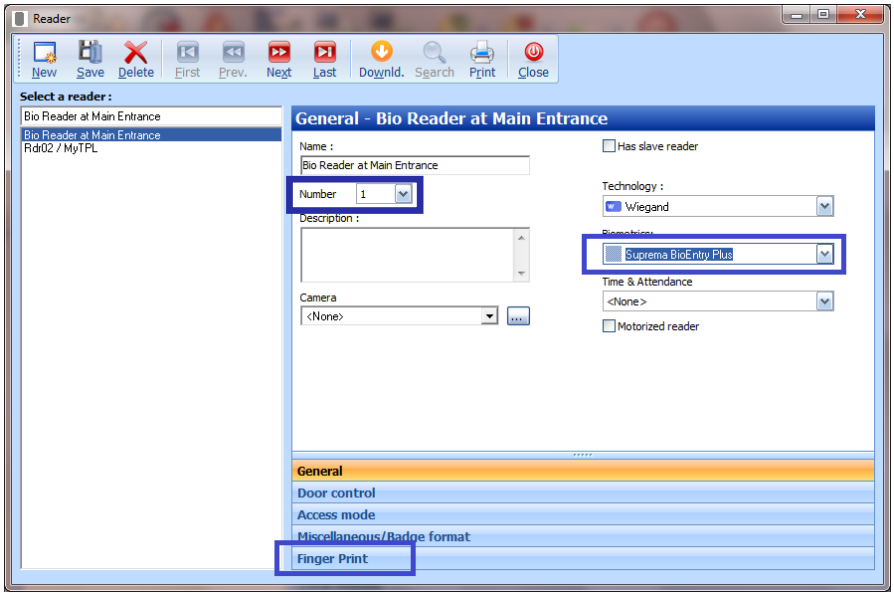
b. In the 'Network' screen create a new network where the biometric reader is connected.
For example if it was allocated (via BioStar) with IP 172.168.1.186, port 1471, the Network setting should be TCP and in the address field type:

172.168.1.186:1471

Give it a logical name that will help you identify it in case there are many network.
For example if the S/N is **36100** you can name the network 'Network for BioReader 36100'.

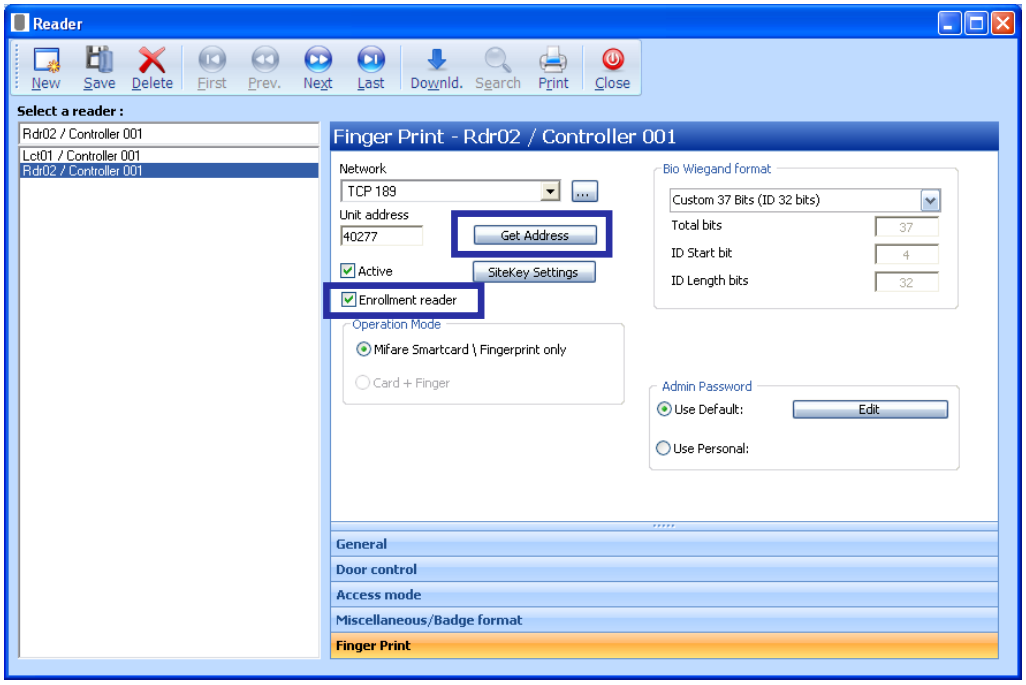


c. In Controller>Reader screen, select the relevant reader.
Important: Mind the value of the reader 'Number'. It should be set 1,2,3 or 4 according to the location on the SENSOR controller where the reader's 'Wiegand Out' was connected. Set the reader type to correct option according to the actual reader model. This will add the 'Finger Print' tab.

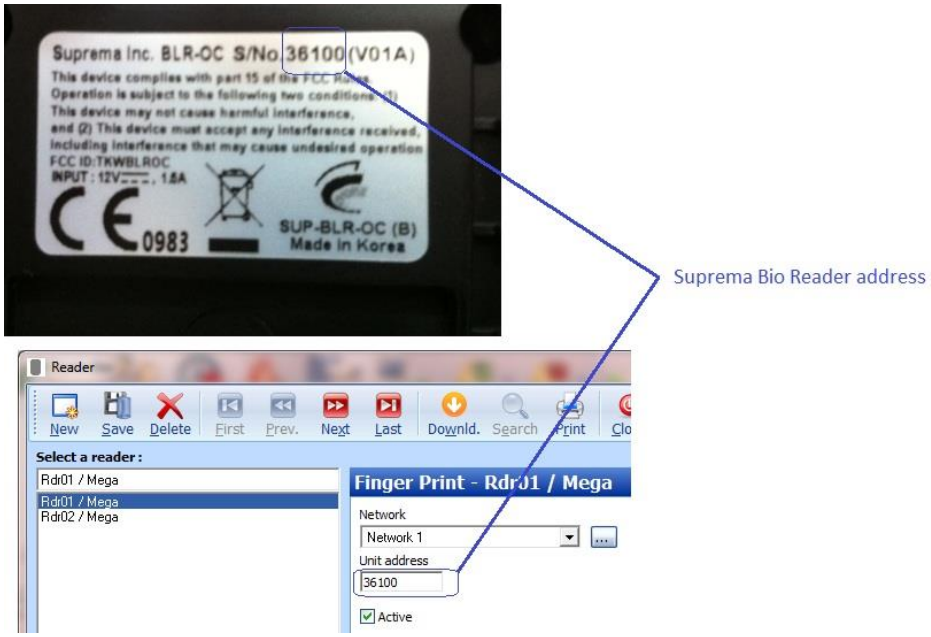


d. Go to the 'Finger Print' tab and select the newly created network (e.g., 'Network for BioReader 36100').
Note: It is not possible to select a Network that is already defined for use by SENSOR controllers.

If the reader is connected to the LAN already, press on the **Get Address** button for detecting automatically the Unit address through the selected Network.
If the reader should be used also for enrollment select the '**Enrollment reader**' option. Any Biometric reader can act as an Enrolment reader (for capturing initial Biometric identity) in addition to its normal function as a regular Access reader. Fingerprint enrolment can be done by a BioMini USB scanner also.
Save.



Note that the Unit address is the S/N printed on a sticker on the reader rear side.



e. Still on this screen, select the Operation Mode of the biometric reader:

1. Configuring the system for Finger Only

Select the '**Mifare Smart Cards \ Fingerprint Only**' option and set the Bio Wiegand Format and the Badge Format as follows:
When working with Finger Only it does not matter which one of the two following reader formats is used in GuardPoint Pro but either format you choose must be consistent on all the readers, biometric and standard, all through the database.
The possible formats are either Hexadecimal, Decimal, Decimal 24 bits, Decimal 6 digits.
Each definition consists of 2 items, as follows:

Hexadecimal

Reader format *(Controller>Reader>Miscellaneous>Badge Format) =* Hexadecimal
Bio Wiegand Format *(Controller>Reader>Finger Print) =* **Custom 37 bits (ID 32 bits)**

Decimal

Reader format *(Controller>Reader>Miscellaneous>Badge Format) =* Decimal**/Decimal 24 bits/Decimal 6 digits**
Bio Wiegand Format *(Controller>Reader>Finger Print) =* **Standard 26 Bits (ID 16 bits)**

2. Configuring the system for Card+Finger with EM-Marine cards

Select the '**Card + Finger**' option and set the Bio Wiegand Format and the Badge Format as follows:
Reader format *(Controller>Reader>Miscellaneous>Badge Format) =* Decimal **24 Bits**
Bio Wiegand Format *(Controller>Reader>Finger Print) =* **Standard 26 Bits (ID 16 bits)**

Notes:

- It is possible to have on the same controller, one reader with the mode 'Fingerprint only' and another with the mode 'Card + Finger'.

- If GuardPoint Pro has been updated from version 2.3.0xx to version 2.4.0xx, make sure that the '**Card + Finger**' option is correctly set for each reader that should work in Card Finger mode.

3. Configuring the system for Card+Finger with Mifare cards

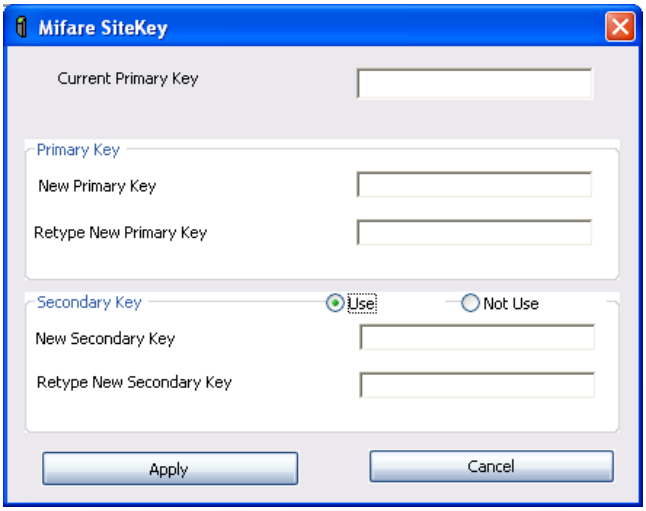
Select the '**Mifare Smart Cards \ Fingerprint only**' option and set the Bio Wiegand Format and the Badge Format as follows:
Reader format *(Controller>Reader>Miscellaneous>Badge Format) =* Hexadecimal
Bio Wiegand Format *(Controller>Reader>Finger Print) =* **Custom 37 bits (ID 32 bits)**

Note: 'Mifare Smartcard' readers require the following GuardPointPro.ini setting in each one of the GuardPoint Pro PCs (server and workstations):

BioStoreTemplateToCard =1

In this case, ALL the biometric readers must be Mifare and also should be configured with the 'Mifare Smartcard' operation mode (the mode Card+Finger is disabled with this setting).

'Mifare Smartcard' readers can be defined with a Site Key, a secret key used to encrypt information sent between Smart Cards and Biometric readers. As a rule, all Biometric readers on the same site should have the same site key. This site key is not stored in the database, for security reasons. So the administrator should remember the key or write it down somewhere. The default site key for Mifare Biometric readers is the empty string. The user can change the key by clicking on **Site Key Settings**. This will open the following screen:



In some cases, if the site key is compromised, it will be need to replace the site key from the old one to a new one. Yet changing the site key will cause all cards with the old site key to fail on entrance. In this case, the administrator should select "**Use**" for entering a Secondary Key, and then enter the old site key. This will allow the selected readers to use both the old and the new site key for a while at the same time. Once all cards are updated with the new site key, the administrator can switch back to a single key by selecting "Not Use" on the Secondary Key section of this screen.
Note that this screen is also available in the Diagnostic screen, at **Download>Change Site Key** (allows multiple selections).

f. Verify the communication with the biometric reader:

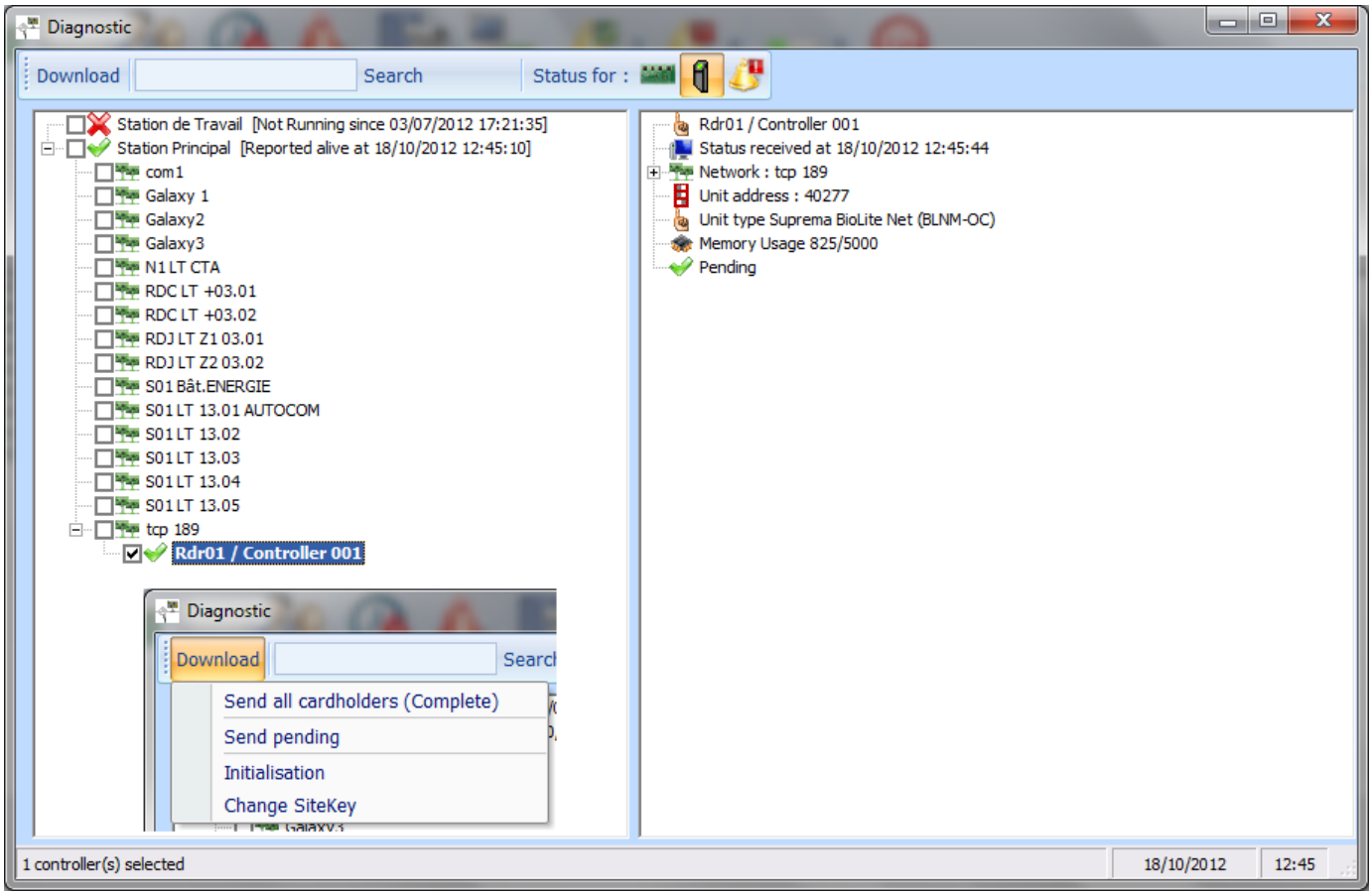
In the Tools>Options>Communication screen, set the Bio baud rate. This baud rate can be different from the controller's baud rate. By default, the baud rate of the Biometric readers is 38400 bauds.

Go to Diagnostics screen, click on '**Biometric Readers**', select the reader on the left window and click on its name. If communication is ok, a green **V** appears on the left to the name.

Now initialize the reader using **Download>Initialization**. Then click again on the reader name and you should see that the Memory Usage is **1/5000**. This first user is the default administrator. Thus the value 1/5000 is normal.

Note that "Unit type" gives information about the specific Biometric reader, i.e. device model, as can be seen on the screen image hereunder.

The **Download>Change Site Key** option is displayed for Sensor biometric readers only. It opens the SiteKey_Settings window for replacing the current Site Key of all the selected biometric readers. At least one reader should be selected before these commands are executed. After clicking "Apply" there will be a popup screen displaying the list of the selected biometric readers - with a green **V** for each reader that has successfully changed its Site Key, and a red **X** for each one that failed.



By expanding the [+] icon on the left to the word 'Network' on the Diagnostics' right window it is possible to view all the communication parameters.

Note that initialization operation is usually needed only in case of inconsistency between the database on the PC and the reader's fingers database. This can happen when replacing a reader but might also occur due to communication problems.
The initialization process performs the following steps:

- Erasing of all the existing finger templates
- Defining an administrator
- Sending the relevant templates from GuardPoint Pro database, according to the cardholders' access groups.

Enrollment process

Since in '**Finger Only**' mode it is possible to work without physical badges, GuardPoint Pro can automatically create virtual badges as part of the enrollment process, saving the user the need to manually define badges.

However, for Biometric readers in '**Card + Finger**' mode, it is not advisable to let GuardPoint Pro create the badge automatically because the user should insert the card code manually to match the actual code on the card. This will be done either by typing in the code or by passing the card and getting the code from a reader.

Thus, in order to support both options, there is an INI entry to control the auto creation:

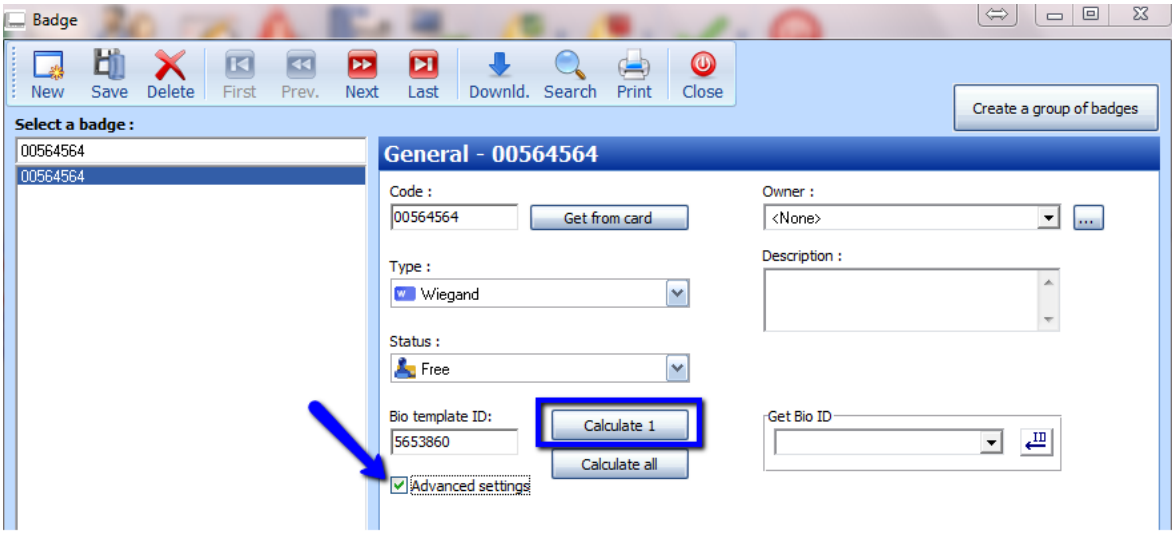
BioCreateBadge = 0; Do not create badges automatically when enrolling.
BioCreateBadge = 1; Card is automatically created and allocated to the relevant cardholder during fingerprint enrolment. It works only for people that did not have card allocated prior to the finger enrollment. Those who did have cards will be left with the same code unchanged.

For Biometric readers in '**Mifare Smartcard**' mode, this possibility depends on the system. See the details in the relevant chapter.

When a finger is enrolled, its template is sent to the Biometric reader with a unique ID. In GuardPoint Pro it is named 'Bio Template ID'.
For cardholders that already had card allocated, it is advisable to make sure that the value at 'Bio Template ID' field in Badge screen is not zero. If it is zero, use the 'Advanced Settings' option and let GuardPoint Pro calculate the 'Bio Template ID'.

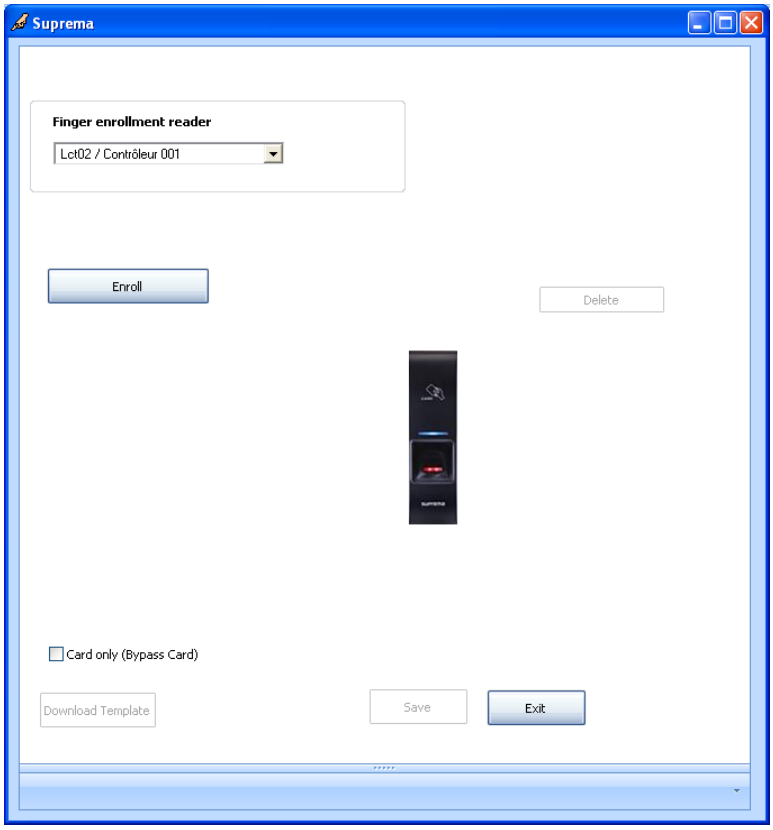
The "Advanced Settings" gives the two following options (see image):
Calculate 1: rebuilds, or creates if zero, the 'Bio Template ID' of the selected card.
Calculate All: rebuilds, or creates if zero, the 'Bio Template ID' of all the cards in the database.

The calculation is based on the card code and the reader format definitions.



Enrollment steps for 'Finger Only' readers

After creating a Cardholder with his access authorization in the "Parameter>All Cardholders>General" screen, click on the '**Biometrics data**' button to open the following enrolment screen.



1. Select the relevant Finger enrolment reader from the list. If the required reader does not appear in the list, open its Reader>"Finger Print" screen and tick the “Enrolment reader” option.
   The Finger enrolment reader may be the USB enrolment reader Bimini. In such case, as soon as Windows detects it, GuardPoint Pro displays an image of the BioMini in this screen and disables the enrolment function from all other readers. Therefore no other readers would appear on the list.
2. Press the ‘**Enrol**’ button for a fingerprint enrolment and follow the instructions displayed on the screen. You will be prompted to put the first finger as long as the yellow LED on the reader blinks.
3. The enrolment process asks for two fingers:
   - Place the first finger and remove it when the blink stops. It usually stops after less than 1 second.
   - Put another finger (or the same finger again). When the yellow blinks stop, remove the finger.
   After the finger enrollment succeeds, a message **"Fingerprint received. Press SAVE before exiting."** is displayed on the screen.
4. Press the ‘**Save**’ button to download the template to the relevant Biometric readers and to save it in the database. The message '**Fingerprint saved**' should appear.
5. When it is needed to delete the current fingerprint press '**Delete**'.
   For re-enrolling the fingerprint, press '**Enrol**'.

If, for any reason, the existing template needs to be re-downloaded to the Biometric readers, press '**Download Template**'.
For using only card identification and not fingerprint scanning (usually for test purposes) check the option **Card only (Bypass card)**.

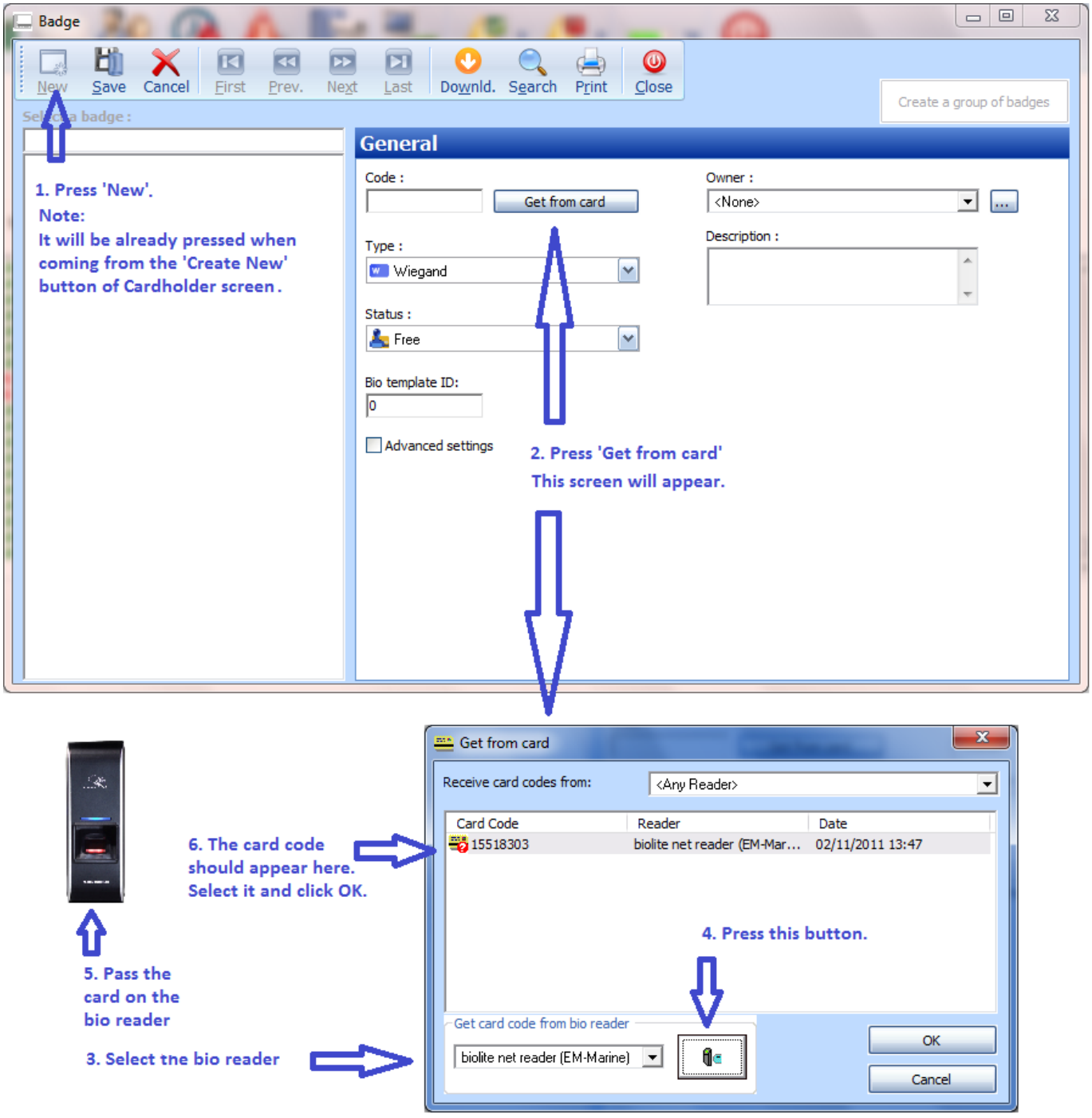
6. Press the '**Exit**' button to close this screen.

Enrollment steps for 'Card + Finger' readers

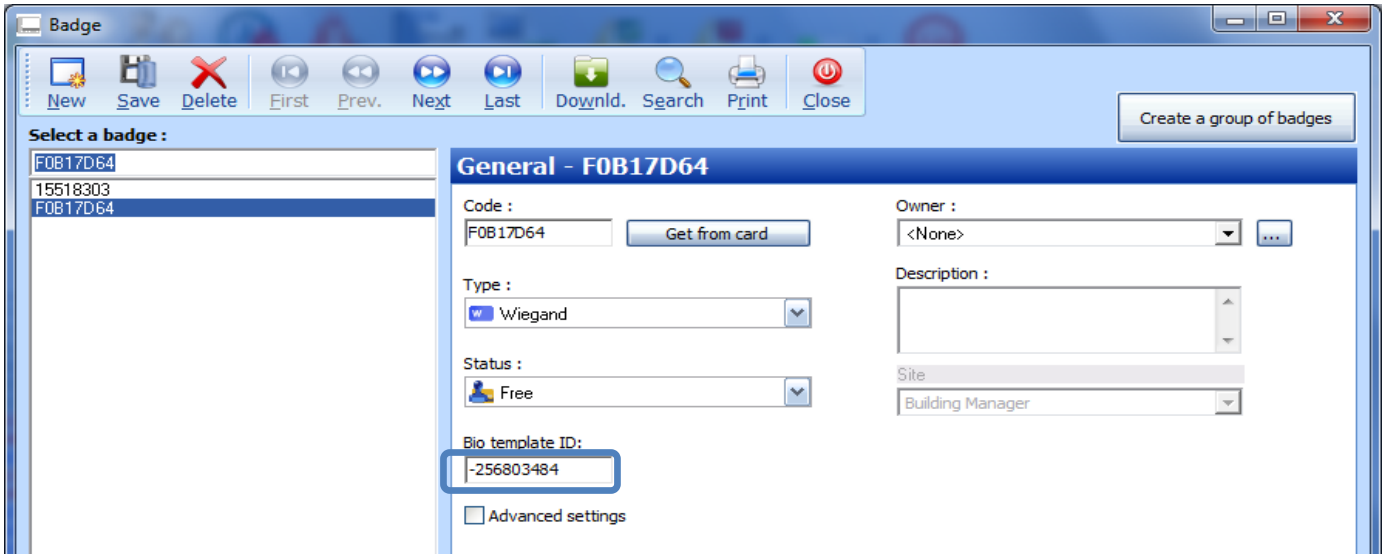
In 'Card + Finger' mode it is required to create the card manually. Therefore set the INI file entry: BioCreateBadge = 0 (Mind that changes in the INI file must be followed by GuardPoint Pro restart).

Allocating a badge to a cardholder may come before or after the finger enrollment. However, it is recommended to start with the badge allocation and enroll the finger afterwards. Only this way the template is sent to the biometric reader already during the enrollment process.

After creating the cardholder and allocating the access group, click on '**Create New**' button to open the 'Badge' screen and follow the step-by-step procedure as shown hereunder (mind the numbers).


Badge
New
Save
Cancel
First
Prev.
Next
Last
Downld.
Search
Print
Close
Create a group of badges
1. Press 'New'.
Note:
It will be already pressed when coming from the 'Create New' button of Cardholder screen.
General
Code :
Get from card
Owner :
<None>
Type :
Wiegand
Description :
Status :
Free
Bio template ID:
0
Advanced settings
2. Press 'Get from card'
This screen will appear.
Get from card
Receive card codes from:
<Any Reader>
Card Code
Reader
Date
15518303
biolite net reader (EM-Mar...
02/11/2011 13:47
6. The card code should appear here. Select it and click OK.
4. Press this button.
5. Pass the card on the bio reader
3. Select the bio reader
Get card code from bio reader
biolite net reader (EM-Marine)
OK
Cancel

1. The 'Bio template ID' should be auto filled by GuardPoint Pro as a conversion of the card code.



Important:

a. The 'Bio Template ID' received by GuardPoint Pro conversion may give a positive or negative values, both are normal. Whatever the auto conversion gives should not be modified.

b. The conversion logarithm is based on the Reader format (Hexadecimal/Decimal/etc.) and the Bio Wiegand Format (Custom 37/Standard 26). All the readers in the database must have the same settings for these 2 items. In case there were wrong definitions in one or more of the readers, then after correcting the definitions you should go back to Badge screen and use the 'Advanced Setting' option to re-calculate the specific card or all the cards. This re-calculation should be done BEFORE the next finger enrolment steps.

2. Save the badge, then save the cardholder. Now click on the '**Biometrics data**' to open the enrolment screen.
3. Select the relevant Finger enrolment reader from the list. If the required reader does not appear in the list, open its Reader>"Finger Print" screen and tick the "Enrolment reader" option.
   The Finger enrolment reader may be the USB enrolment reader BioMini. In such case, as soon as Windows detects it, GuardPoint Pro displays an image of the BioMini in this screen and disables the enrolment function from all other readers. Therefore no other readers would appear on the list.
4. Press the '**Enrol**' button for a fingerprint enrolment and follow the instructions displayed on the screen. You will be prompted to put the first finger as long as the yellow LED on the reader blinks.

5. The enrolment process asks for two fingers:
   - Place the first finger and remove it when the blink stops. It usually stops after less than 1 second.
   - Put another finger (or the same finger again). When the yellow blinks stop, remove the finger.
   After the finger enrollment succeeds, a message **"Fingerprint received. Press SAVE before exiting."** is displayed on the screen.
6. Press the '**Save**' button to download the template to the relevant Biometric readers and to save it in the database. The message '**Fingerprint saved**' should appear.
7. When it is needed to delete the current fingerprint press '**Delete**'.
   For re-enrolling the fingerprint, press '**Enrol**'.
   If, for any reason, the existing template needs to be re-downloaded to the Biometric readers, press '**Download Template**'.
   For using only card identification and not fingerprint scanning (usually for test purposes) check the option **Card only (Bypass card)**.
8. Press the '**Exit**' button to close this screen.

Enrollment steps for 'Mifare Smartcard' readers

Requirements:

'Mifare Smartcard' readers require the following GuardPoint Pro.ini setting in each one of the GuardPoint Pro PCs (server and workstations):

BioStoreTemplateToCard =1

In this case, ALL the biometric readers must be Mifare and also should be configured with the 'Mifare Smartcard' operation mode in the Reader/Finger Print screen.

The enrolment process is different with Mifare Smart Card readers because with theses readers, the templates are stored into Smart Cards.
This has 2 advantages:
- No personal data is stored on the computer or on the reader
- The total number of finger templates is unlimited

Regarding the "BioCreateBadge" INI option, its value depends on whether or not the cardholders already have an allocated card.

1. **Installations where cardholders do not have an allocated card yet**

In such a case it is recommended to set the GuardPoint Pro.ini entry:

BioCreateBadge = 1

Thus, GuardPoint Pro automatically creates the card as part of the enrolment process.
The created card code is the Card Serial Number (CSN) of the Smart Card, and thus the same card can be used at standard Mifare card readers (i.e., Mifare readers for card only).

Important: As said above, this method is suitable for cardholders that do NOT have an allocated card yet. However, it might be that some cardholders in the database already have an allocated card.
For them we distinguish between two scenarios:

a. The existing allocated code **equals** the CSN of the card that is about to store the finger template.
In this case the enrolment should be possible without changing the existing card.

b. The existing allocated code is **different** from the CSN.
In this case you must remove the card (and save) before starting the enrolment process.

2. **Installations where cardholders already have an allocated card**

The GuardPoint Pro.ini entry in this case should be:

BioCreateBadge = 0

With this setting the biometric readers use the 'Bio Template ID' of the allocated card.
This 'Bio Template ID' is later sent to the Smart Card as part of the enrolment process.

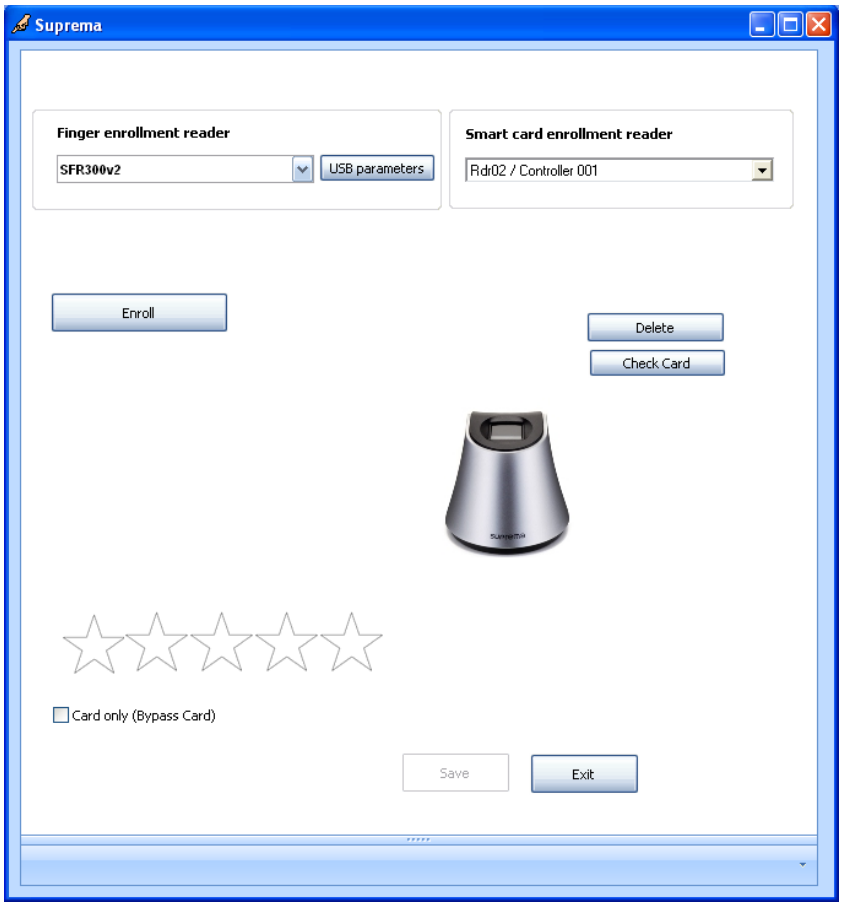
Be aware of two possible problems:

a. The value at 'Bio Template ID' field of an existing card is zero.
In such a case no template will be sent and the enrolment cannot succeed.

b. Finger pass gives "Unknown card" event.
This happens due to wrong matching of the card code and the 'Bio Template ID'.

The solution to both points is the same: You need to recalculate the 'Bio Template ID'.
This is done with the "Advanced Settings" in Badge screen (see above).

Warning: With the INI entry BioCreateBadge = 0 the enrolment process expects that each cardholder would have an allocated card. In case no card is allocated - the enrolment process would stop.
After creating a new cardholder with his access authorization in the "Parameter>All Cardholders>General" screen, click on the '**Biometrics data**' button to open the following enrolment screen.



The system requires two readers for the enrolment: one reader for the finger enrolment and another for the Smart Card enrolment.

1. Select the relevant enrolment readers from each list. If the required reader does not appear in the list, open its Reader>"Finger Print" screen and tick the “Enrolment reader” option.
   The Finger enrolment reader may be the USB enrolment reader BioMini. In such case, as soon as Windows detects it, GuardPoint Pro displays an image of the BioMini in this screen and disables the enrolment function from all other readers. Therefore no other readers would appear on the ‘Finger enrolment reader’ list.
2. Press the ‘**Enrol**’ button for a fingerprint enrolment and follow the instructions displayed on the screen. You will be prompted to put the first finger as long as the yellow LED on the reader blinks.
3. Finger enrolment step:
   The enrolment process asks for two fingers:
   - Place the first finger and remove it when the blink stops. It usually stops after less than 1 second.
   - Put another finger (or the same finger again). When the yellow blinks stop, remove the finger.
   After the finger enrollment succeeds, a message **"Fingerprint received. Press SAVE before exiting."** is displayed on the screen.
4. Smart Card enrolment step:
   Press ‘**Save**’ and present an empty Smart Card at the Smart Card enrollment reader.
   Follow the instructions on the screen. After the Smart Card enrollment succeeds, there should be a message "**Template stored in card successfully.**".
5. Press the '**Exit**' button to close this screen.

Deleting a template from the Smart Card:
When it is needed to delete the existing finger print template from a Smart Card press '**Delete**' and present the Smart Card at the Smart Card enrollment reader.

Replacing an existing finger print template on the Smart Card:
Use the ‘**Enrol**’ button.

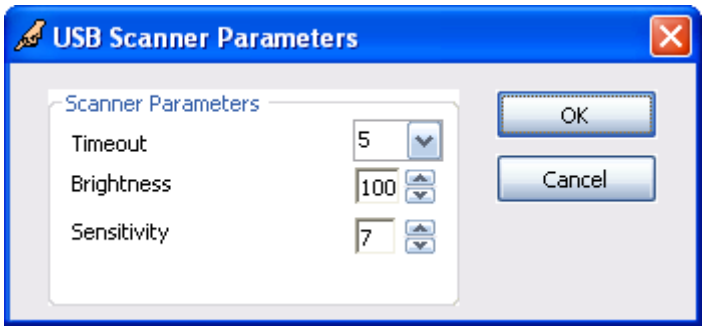
Allowing pass with card only (without a finger):
For using card-only identification (usually for test purposes) select the option:
’**Card only (Bypass card)**’.

Notes:

- During the enrolment process, if it is detected that Smart Card already carries a fingerprint, the user is asked whether to keep the existing template or to overwrite it with the new one.

Mind that it is possible to verify that the card is empty before the enrolment process using the '**Check Card**' option. When this check finds that the card is not empty, the message "**Smartcard contains fingerprints**" would be displayed. Then you can use the "**Delete**" button to empty the Smart Card.

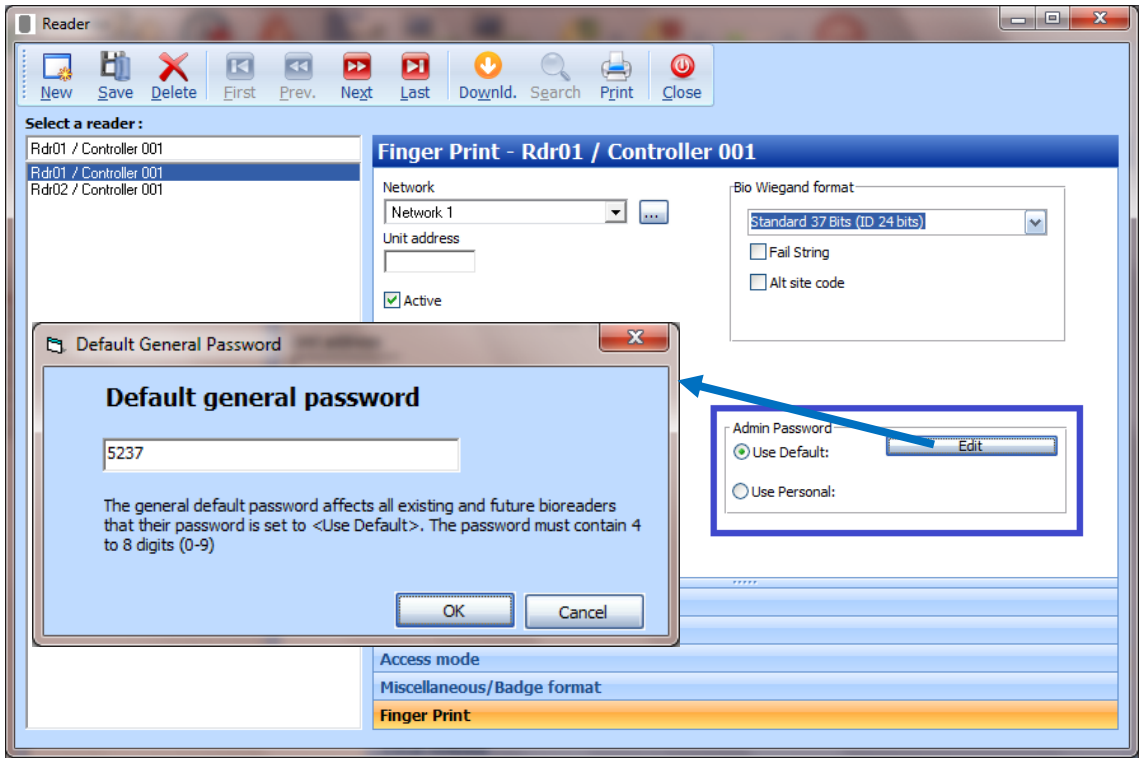
- When using the **BioMini**, the '**USB parameters**' button enables fine tuning of the following BioMini scanner settings: Timeout, Brightness, and Sensitivity.



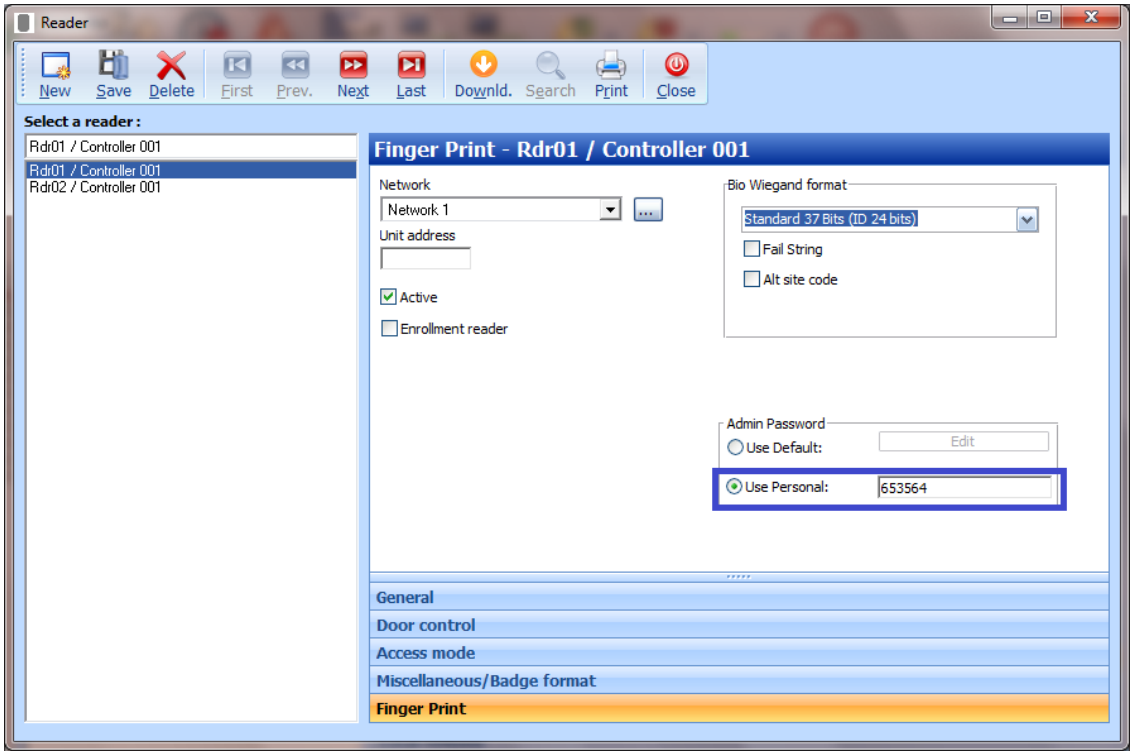
- On exiting the 'Biometric Data' screen, GuardPoint Pro saves the user selection of the readers for the next time this screen is opened.

Reader Administrator Password

On **S-Bio-KP** (the reader with the keypad) there must be at least one Administrator with a defined password in order for the reader to function and accept fingers. Therefore GuardPoint Pro database has a general default password for all Sensor readers. This password can be edited by the user at the reader screen at Finger Print tab. The password must contain between 4 and 8 decimal digits.



It is also possible to set a reader to have a specific password different from the general password. This is done by selecting the '**Use Personal**' option and then, enter the password in the field.



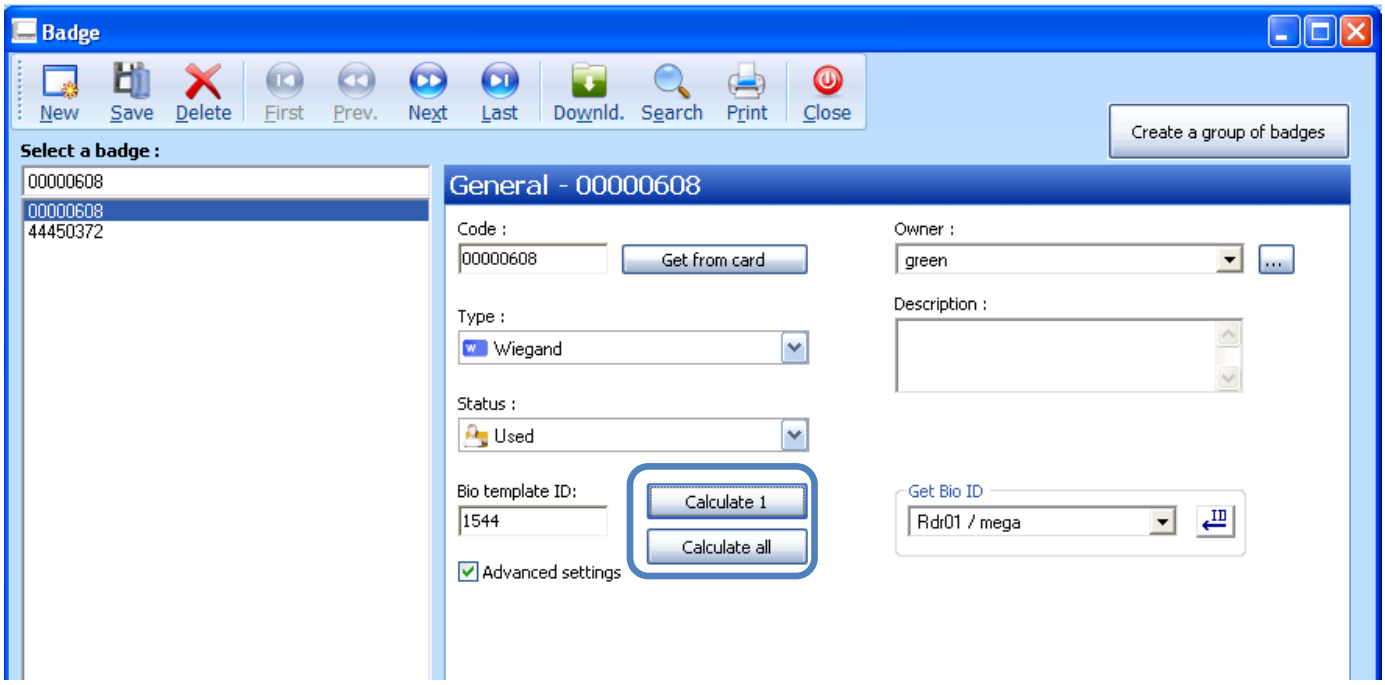
Calculating the 'Bio Template ID'

Each template needs to be downloaded to the biometric readers with an identification number (called 'Bio Template ID'), which identifies the person. GuardPoint Pro auto calculates the 'Bio Template ID' and fills the corresponding field in Badge screens. The 'Bio Template ID' is normally automatically computed by the system from the card code, based on the Badge format (defined in the *Reader>Miscellaneous>Badge format* tab) and the Bio Wiegand format (defined in the *Reader>Finger Print* tab).

However, in a case where the database already contains cardholders **prior** to the addition of the Sensor readers, 'Bio Template ID' of these cardholders will stay '0'. The value of zero is not acceptable by the reader. In such cases it is required to force GuardPoint Pro to calculate the 'Bio Template ID'. This is done by using the '**Advanced Setting**' option in Badge screen.

Selecting the option reveals 2 buttons: 'Calculate' & 'Calculate All'.

- **Calculate** → Calculates the 'Bio Template ID' for the selected cardholder
- **Calculate All** → Calculates the 'Bio Template ID' for all the cardholders in the database



This calculation should be done after all the readers were defined and their two formats ('Reader Format' & 'Bio Wiegand Format') were configured according to the one of the three modes as explained above. For your convenience here's a summary of the 3 working modes and their relevant format settings:

Operation Mode	Reader Format	Bio Wiegand Format
Fingerprint Only option 1	Decimal	Standard 26 Bits
Fingerprint Only option 2	Hexadecimal	Custom 37 bits
Card + Finger	Decimal	Standard 26 Bits
Mifare Smart Cards	Hexadecimal	Custom 37 bits