GuardPointPro - Denied access events supported on SUPREMA Bio Readers

Introduction

This document describes how to receive the denied access events from Suprema readers.
This feature consists to configure the biometric readers in order to send a specific code to the controller in case of denial.
The controller interprets this code and sends the corresponding denied transaction to GuardPointPro

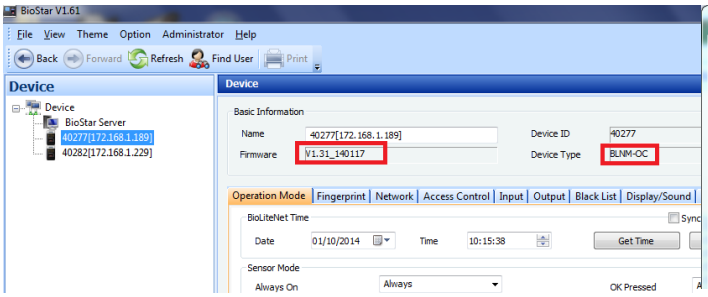
Requirements

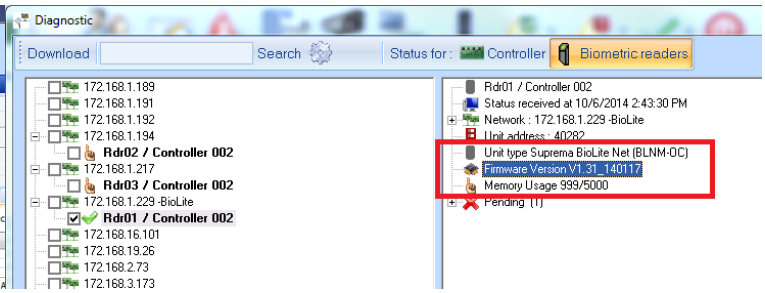
This feature requires GuardPointPro version 3.0.033 or later.
The controller firmware must be from: 03/04/2014 or later for IC2000/2001/4000/4001
07/04/2014 or later for IC-Pro 2/4

The Bio reader firmware must be as follows:

Bio Reader	 BioEntry Plus				 BioEntry W			 BioLite Net	
Card Type	125kHz EM card	Mifare (13.56MHz)	HID Prox.	iClass (13.56MHz)	Mifare (13.56MHz)	HID Prox.	iClass (13.56MHz)	125kHz EM card	Mifare (13.56MHz)
Model	**BEPL-OC**	**BEPM-OC, BEPM-TC**	**BEPH-OC**	**BEPI-OC**	**BEWM**	**BEWH**	**BEWI**	**BLR-OC**	**BLNM-OC**
Firmware	**V1.6_140314**	**V1.62_170406**	NA	NA	NA	**V1.2_140314**	NA	NA	**V1.31_140117**

[You can download all special firmware from here]
Use Biostar to upload the correct firmware
The firmware version may be checked either in the BioStar screen, or in the Diagnose screen of GuardPointPro from version 3.1.027.





CAUTION: If one of the firmware version or the software version is not correct please contact us.

GuardPointPro - Denied access events supported on SUPREMA Bio Readers

Description

On denied accesses from the Bio reader, GuardPointPro displays the denied events on the log event screen with a specific denied reason.
For example, if a cardholder named 'Bill' presents his card at the Bio Reader with a wrong finger, GuardPointPro will display the following event: 'Access Denied 'Bill' - Card known but finger unknown'

The specific denied reason may be different following to situation:

Situation	Corresponding denied reason in GPP
in Finger-only mode	
The presented card is not in the system.	**Unknown Card**
The presented card does not belong to anyone.	**Non Allocated Badge**
The presented card is not authorized at this reader.	**Access Group**
Unrecognized finger is presented. In this case, the code "9999" is sent and GPP receives 'Unknown card '00009999' '. To display the message "Unrecognized finger", the user should previously create a cardholder with the card code "00009999".	**Unrecognized finger**
The presented card belongs to someone but it is not in the reader memory.	**Card not in reader memory**
The presented card is stored in the reader memory with another finger.	**Card with wrong finger**
in Card + Finger mode	
The presented card is not in the system.	**Unknown Card**
The presented card does not belong to anyone.	**Non Allocated Badge**
The presented card is not authorized at this reader.	**Access Group**
The presented card belongs to someone but it is not in the reader memory.	**Card not in reader memory**
The presented card is stored in the reader memory with another finger.	**Card with wrong finger**
A finger has been presented before the card whereas a card is required first. In this case, the code "9999" is sent and GPP receives 'Unknown card '00009999' '. To display the message "Card is required first", the user should previously create a cardholder with the card code "00009999".	**Card is required first**
When finger template are stored on Smartcard only (INI option BioStoreTemplateToCard = 1)	
The presented card is not in the system.	**Unknown Card**
The presented card does not belong to anyone.	**Non Allocated Badge**
The presented card is not authorized at this reader.	**Access Group**
A finger has been presented before the card whereas a card is required first. In this case, the code "9999" is sent and GPP receives 'Unknown card '00009999' '. To display the message "Unrecognized finger", the user should previously create a cardholder with the card code "00009999".	**Unrecognized finger**
The presented Smartcard does not contain any template. Note that if the card does not exist in the controller memory, GPP receives an "Unknown card" event instead.	**Empty smart card**
The presented Smartcard contains a template of another finger.	**Smart card with wrong finger**

GuardPointPro - Denied access events supported on SUPREMA Bio Readers

Example 1: if a card code is not in the reader memory, GuardPointPro will display the denied reason 'Card unknown'.

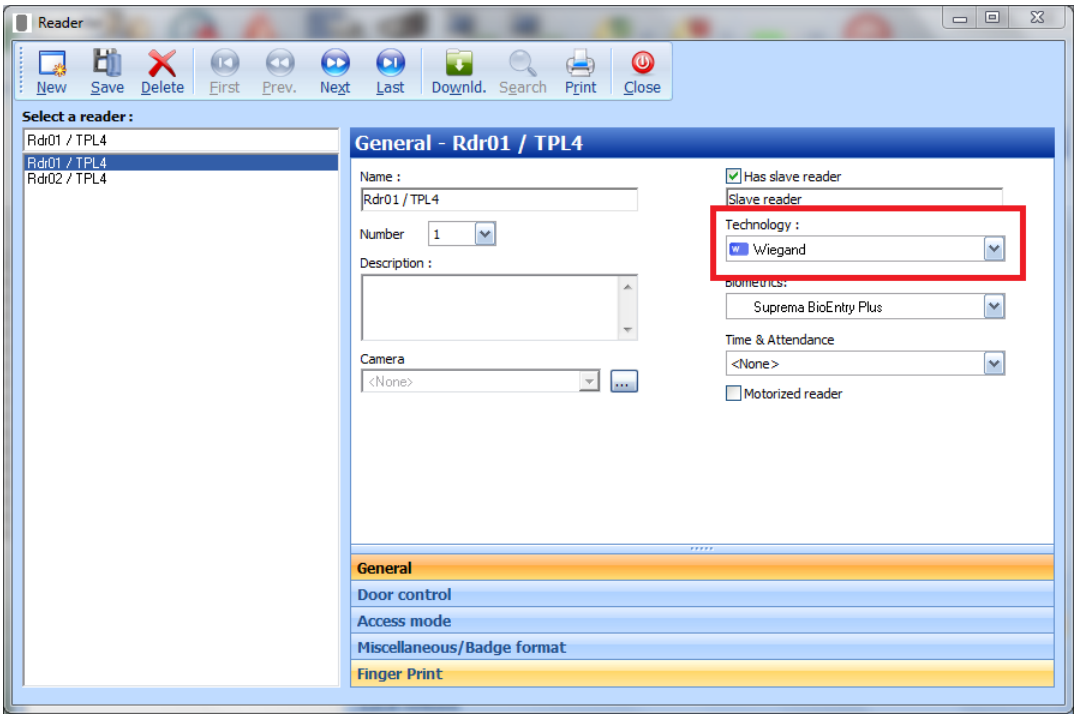
Example 2: if a card code is in the reader memory but presented with a wrong finger, GuardPointPro will display the denied reason 'Card known but finger unknown'.

Example 3: upon unrecognized finger, GuardPointPro will display 'Unknown card 00009999'.
If creating for example a cardholder with the name "Error" and the card code "00009999", upon unrecognized finger the message will be: 'Access Denied 'Error' - Unknown finger'.

Example 4: therefore, if a finger has been presented before the card in the Card+Finger mode, GuardPointPro will display 'Unknown card 00009999'.
If creating for example a cardholder with the name "Error" and the card code "00009999", when a finger is presented before the card in the Card+Finger mode, the message will be: 'Access Denied 'Error' - Finger is passed without a card'.

Configuration in GuardPointPro

1- The reader should be configured with the Technology "Wiegand" in the 'Reader > General' screen.

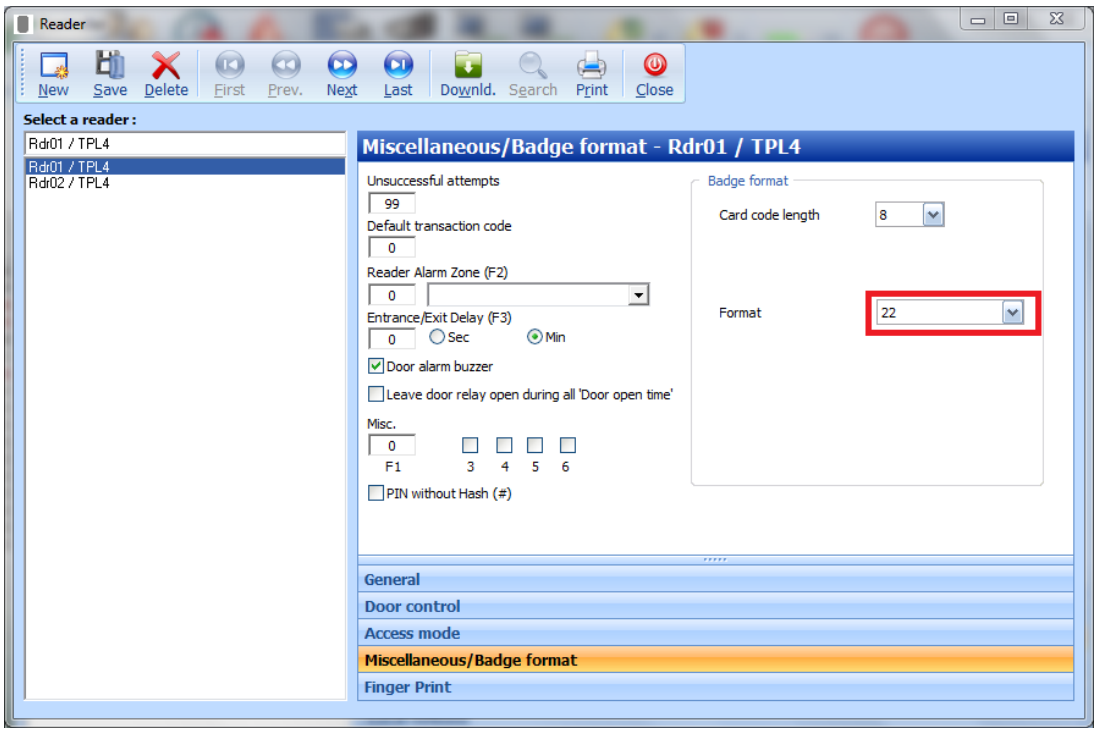


GuardPointPro - Denied access events supported on SUPREMA Bio Readers

2- Following to the card format, the Badge format and the Bio Wiegand Format must be as follows:

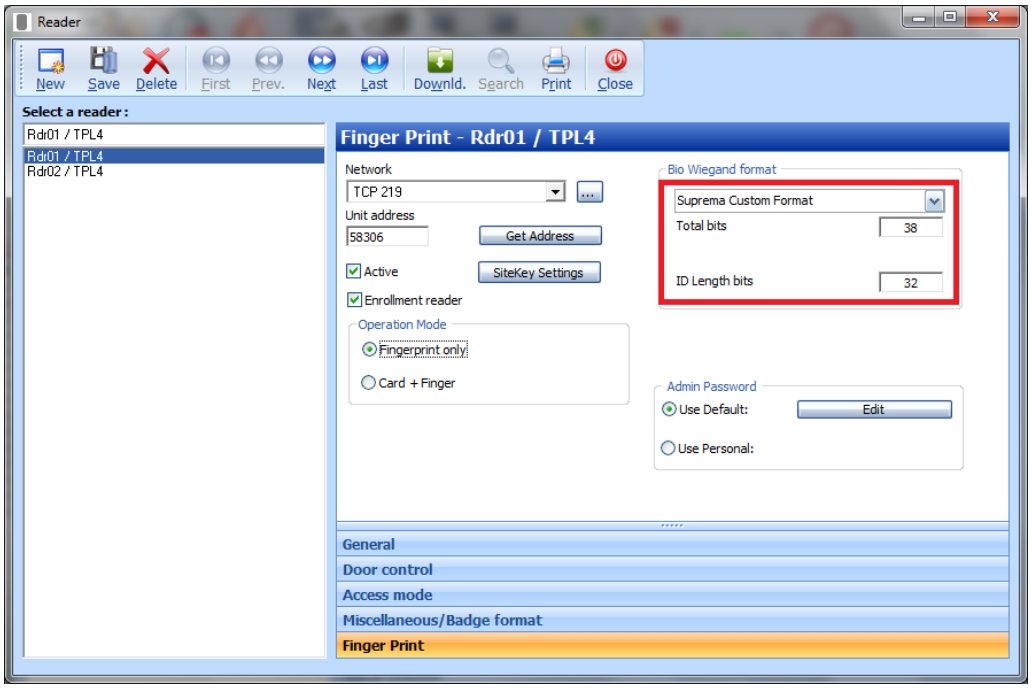
Card Format	Card code length	Badge Format	Bio Wiegand Format: Suprema Custom Format
34 bits ex. A3361126	8	22	Total bits: 38 ID Length bits: 32
37 bits ex. 780AB689F	8	23	Total bits: 38 ID Length bits: 32
26 bit ex. 001A2B3C	8	24	Total bits: 26 ID Length bits: 16

3- The reader should be configured with the right Badge format in the 'Reader > Miscellaneous/Badge format' screen.
Hereunder an example when using 34 bits cards; following to the previous table the Badge Format should be '22' and the card code length should be '8'.



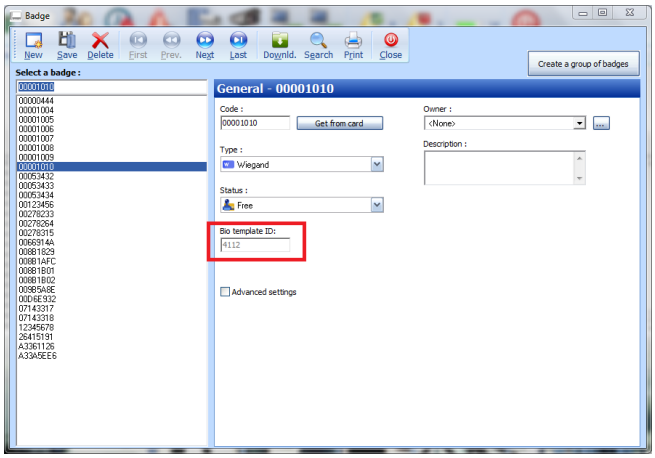
GuardPointPro - Denied access events supported on SUPREMA Bio Readers

4- The reader should be configured with the right Bio Wiegand Format in the ‘Reader > Finger Print’ screen.
Hereafter an example when using 34 bits cards; following to the previous table the Bio Wiegand Format should be ‘Suprema Custom Format’, Total bits: 38 and ID Length bits: 32.



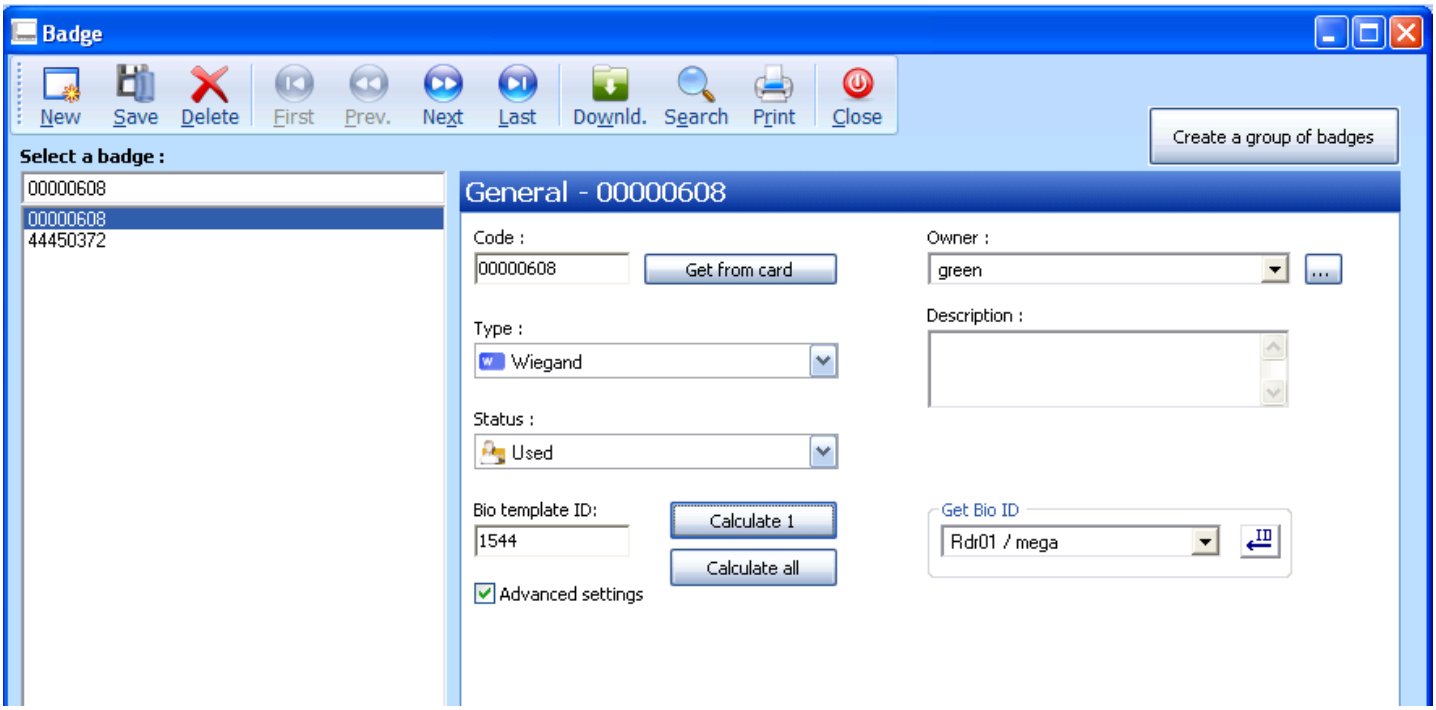
5- A cardholder must be created with the name “Error” for example and the card code "00009999".

Note that it is important that the ‘Bio Template ID’ of the cards is not equal to 0. To check it, open the Badge screen and look at the corresponding field.



GuardPointPro - Denied access events supported on SUPREMA Bio Readers

The 'Bio Template ID' is normally automatically computed by the system from the card code, based on the Badge format and the Bio Wiegand format.
However, in a case where the database already contains cardholders prior to the addition of the Suprema 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 GuardPointoPro 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 above table.