

BioEntry™ Operation Manual

BioEntry™ Smart / Pass

Ver. 0.95

Suprema Inc. and BioEntry™ are registered trademarks of Suprema Inc. All rights reserved. No part of this work covered by the copyright hereon may be reproduced or copied in any form or by any means – graphics, electronic, or mechanical, including photocopying, recording, taping, or information and retrieval systems – without written permission of Suprema Inc. Any software furnished under a license may be used or copied only in accordance with the terms of such license.

Suprema Inc reserves the right to modify or revise all or part of this document without notice and shall not be responsible for any loss, cost or damage, including consequential damage, caused by reliance on these materials.



Copyright © 2005 by Suprema Inc.

Suprema Warranty Policy

Suprema warrants to buyer, subject to the limitations set forth below, that each product shall operate in substantial accordance with the published specifications for such product for a period of one (1) year from the date of shipment of the products ("Warranty Period"). If buyer notifies Suprema in writing within the Warranty Period of any defects covered by this warranty, Suprema shall, at its option, repair or replace the defective product which is returned to Suprema within Warranty Period, freight and insurance prepaid by buyer. Such repair or replacement shall be Suprema's exclusive remedy for breach of warranty with respect to the Product. This limited warranty shall not extend to any product which has been: (i) subject to unusual physical or electrical stress, misuse, neglect, accident or abuse, or damaged by any other external causes; (ii) improperly repaired, altered or modified in any way unless such modification is approved in writing by the Supplier; (iii) improperly installed or used in violation of instructions furnished by Suprema.

Suprema shall be notified in writing of defects in the RMA report supplied by Suprema not later than thirty days after such defects have appeared and at the latest one year after the date of shipment of the Products. The report should give full details of each defected product, model number, invoice number and serial number. No product without RMA (Return Material Authorization) number issued by Suprema may be accepted and all defects must be reproducible for warranty service.

Except as expressly provided herein, the products are provided "as is" without warranty of any kind, either express or implied, including, but not limited to, warranties or merchantability, fitness for a particular purpose.

Disclaimers

Information in this document is provided in connection with Suprema products. No license, express or implied, by estoppels or otherwise, to any intellectual property rights is granted by this document. Except as provided in Suprema's Terms and Conditions of Sale for such products,

Suprema assumes no liability whatsoever, and Suprema disclaims any express or implied warranty, relating to sale and/or use of Suprema products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right.

Suprema products are not intended for use in medical, life saving, life sustaining applications, or other applications in which the failure of the Suprema product could create a situation where personal injury or death may occur. Should Buyer purchase or use Suprema products for any such unintended or unauthorized application, Buyer shall indemnify and hold Suprema and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Suprema was negligent regarding the design or manufacture of the part.

Suprema reserves the right to make changes to specifications and product descriptions at any time without notice to improve reliability, function, or design. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Suprema reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them.

Please contact Suprema, local Suprema sales representatives or local distributors to obtain the latest specifications and before placing your

product order.

Note: Third-party brands and names are the property of their respective owners.

About the BioEntry™ Series

BioEntry™ is an advanced biometric access reader equipped with award winning fingerprint recognition engine and standard wiegand interface. BioEntry™ can practically replace legacy and simple readers and be instantly added onto existing access control systems as well as new installations.

BioEntry™ Smart is a fingerprint smart card reader that seamlessly integrates fingerprint and smart card reader into one device. BioEntry™ Smart is designed to replace existing access readers like proximity or magnetic readers without additional wiring. Fingerprint template is stored in each user's smart card and there is no need to store fingerprint data in a reader itself. This eliminates the burden of template management and networking readers.

BioEntry™ Pass is a fingerprint access reader equipped with fast one to many fingerprint identification engine. Enrolled with more than hundreds of users, identification can be done in less than one second.

Following the unique feature of Suprema's famous UniFinger™ fingerprint identification modules, BioEntry™ also provides customers with multiple choices of fingerprint sensors including optical, capacitive and thermal sensors.

About Suprema Inc

Suprema is a leading biometric company offering core fingerprint technologies for embedded and PC applications. Suprema's fingerprint products include low cost standalone OEM modules, access control readers, USB fingerprint scanners and fingerprint algorithm SDK.

Suprema's fingerprint recognition algorithm was proved to be world top level by ranking first in the 3rd international Fingerprint Verification Competition (FVC2004) with the lowest error rate in light category. Suprema's fingerprint products have been sold to more than 50 different countries and are being used in various applications.

For more information on Suprema's technologies and products, Please visit Suprema's website (<http://www.supremainc.com>) or contact by e-mail (sales@supremainc.com).

About This Manual

This is an introduction to operation of BioEntry™ Smart and Pass. This guide describes how to do template management of respective BioEntry, properly adjust relevant parameters, enroll or delete templates, etc. The purpose of this manual is to provide instructions on using BioEntry™ Smart and Pass and trouble shooting minor problems.

Contents

Contents.....	6
1. Getting Started	9
1.1. Networking BioEntry	9
1.2. Security Setting	9
1.3. Configuration of BioEntry	9
1.4. Management of User Database.....	10
2. Networking BioEntry's.....	11
2.1. Check Status	11
2.2. Add Group	11
2.3. Rename Group	11
2.4. Remove Group.....	11
2.5. Search Reader	11
2.6. Rename Reader	11
2.7. Remove Reader.....	11
2.8. Change Group	11
3. User Management	12
3.1. Current.....	12
3.2. Synchronize Selected User Templates	12
3.3. Host User Database	12
3.4. Register New User.....	12
3.5. Handling smartcard.....	13
3.6. Import User	14
3.7. Selection Tool	14
3.8. Export Selected User	15
3.9. Delete Selected User.....	15
4. Log Management.....	16
4.1. Current.....	16

4.2. Upload Log	16
4.3. Set Time.....	16
4.4. Host Log Data	16
4.5. Filtering Tool.....	16
4.6. Export Selected Log Data	17
4.7. Delete Selected Log Data	17
4.8. Upload Log Data from Command Card	17
5. Command Card	18
5.1. Command Card List.....	18
5.2. Read Command Card	18
5.3. Issuance Command Card	18
6. Parameter Configuration.....	22
6.1. Current Configuration.....	22
6.2. Fill with Current Configuration Value.....	22
6.3. Apply	22
6.4. Operation Mode	22
6.5. Security Level	22
6.6. Image Quality	23
6.7. Sensitivity	23
6.8. Scan Timeout	23
6.9. Matching Timeout.....	23
6.10. Fast Mode	23
7. I/O Configuration	24
7.1. Current Configuration.....	24
7.2. Fill with Current Configuration Value.....	24
7.3. Apply	24
7.4. Input port setting.....	24
7.5. Output port setting.....	24
8. LED/Beep Control	26

8.1. Current Configuration.....	26
8.2. Fill with Current Configuration Value.....	26
8.3. Apply	26
8.4. Red, Green LED setting	26
8.5. Beep setting.....	26
9. Wiegand Configuration	28
9.1. Current Configuration.....	28
9.2. Fill with Current Configuration Value.....	28
9.3. Apply	28
9.4. Set Configuration	28
9.5. Format.....	28
9.6. Pulse	29
9.7. Wiegand Format File	29
10. Smartcard Layout.....	36
10.1. Current Card Layout.....	36
10.2. Fill with Current Configuration Value	36
10.3. Apply.....	36
10.4. New Card Layout.....	36
11. Preference.....	38
11.1. Com Port.....	38
11.2. Admin Password.....	38
11.3. Site Key Setting.....	39
11.4. Default Backup Directory.....	40
12. Firmware Upgrade	41
12.1. Search Firmware & Upgrade.....	41

1. Getting Started

This manual illustrates how to operate BioEntry™ Smart and Pass using BioEntry Admin software. BioEntry™ Admin is a software running on Windows based PC platforms and designed to communicate with BioEntry™ Smart and Pass. To use BioEntry™ Admin software, BioEntry™ Smart and Pass should be connected to the host computer by RS232/RS422/RS485 network. Refer to BioEntry™ Installation Guide for the details of hardware connection.

This manual covers the following functions of BioEntry™ Admin software.

1.1. Networking BioEntry

BioEntry can be connected through RS232/RS422/RS485 network line.

- To select the COM port of a host computer which is connected to BioEntry, please refer to Section 11.1. Com Port
- To search all connected BioEntry's through the selected COM port automatically, please refer to Section 2.5. Search Reader.
- To divide multiple BioEntry readers into several groups, please refer to Section 2.2. Add Group

For BioEntry Smart series, there is an option to use a command card to directly control BioEntry without connecting to a host computer. Please refer to Chapter 5. Command Card.

1.2. Security Setting

- To enhance security, BioEntry Admin software can lock BioEntry when the software is closed. If BioEntry is locked, BioEntry Admin software asks administrator's password when the software begins. If a wrong password is entered, BioEntry will remain locked. Execute 'Check Status' and enter a correct password to unlock BioEntry. Please refer to section 2.1. Check Status and section 11.2. Admin Password
- For BioEntry Smart series, the site key of BioEntry must be changed at first and a user should remember it. Please refer to Section 11.3. Site Key Setting.

1.3. Configuration of BioEntry

BioEntry can be configured depending on the circumstances.

- To change the parameter such as security level, timeout, please refer to Chapter 6. Parameter Configuration.

- To change the general input and output configuration, please refer to Chapter 7. I/O Configuration.
- To change the LED status and beep sound of BioEntry, please refer to Chapter 8. LED/Beep Control.
- To change the Wiegand format, please refer to Chapter 9. Wiegand Configuration.

For BioEntry Smart series, if the layout of a smart card is different from default layout, the layout of a smart card should be changed before issuing a user smart card. To change the layout of smart card, please refer to Chapter 10. Smartcard Layout.

1.4. Management of User Database

User database of BioEntry Admin software includes user information and fingerprint template.

- To add a new user in user database, please refer to Section 3.4. Register New User.
- For BioEntry Smart series, user fingerprint template should be stored in a smart card. Please refer to Section 3.5. Handling smartcard.

2. Networking BioEntry's

2.1. Check Status

Check the status of BioEntry readers. If the BioEntry reader is connected now, the icon of each reader is highlighted. Otherwise, it remains grayed.

2.2. Add Group

Add new group of BioEntry readers.

2.3. Rename Group

Give a different name on the respective group. Same names cannot be used for different groups.

2.4. Remove Group

Remove a selected group. In order to remove a specific group, it is necessary to remove all BioEntry readers inside the group.

2.5. Search Reader

Search BioEntry readers connected at present.

2.6. Rename Reader

Change a name of a BioEntry reader. The BioEntry reader ID which is indicated in a bracket [] is fixed and cannot be changed.

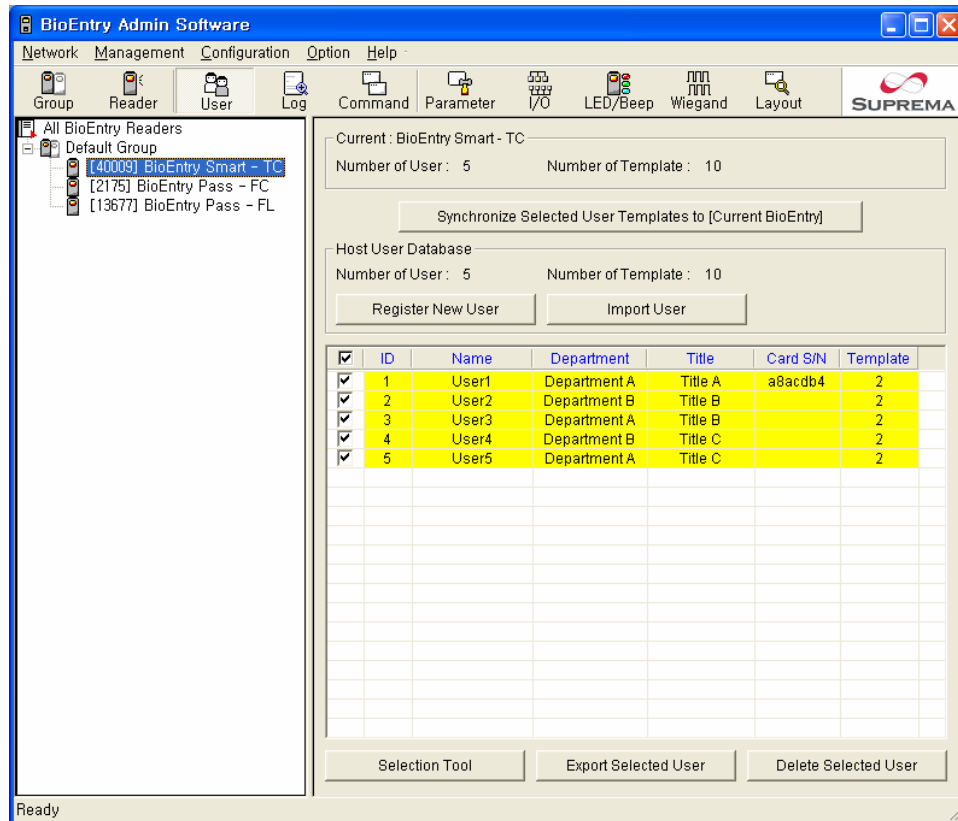
2.7. Remove Reader

Remove a selected BioEntry reader.

2.8. Change Group

To change groups of BioEntry readers, simply drag & drop a reader icon to a different group that you want to move.

3. User Management



3.1. Current

This shows the number of users and templates saved in the currently selected BioEntry. No information is shown if a group or all BioEntry readers are selected.

3.2. Synchronize Selected User Templates

Synchronize selected user templates of the user list to all BioEntry readers, current group, or current BioEntry. If there are some remaining templates in BioEntry, which are not in a database of a host PC or not selected, user can choose options to delete or keep those templates left.

3.3. Host User Database

Display the number of users and templates saved in a database of a host PC.

3.4. Register New User

Register a new user by adding user information such as user ID, user name, and fingerprint template.

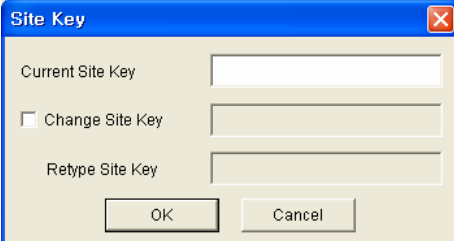
If you want to change the information of existing user, just double-click user in the list.

- Use BioEntry as Enroll Station – If this option is selected, BioEntry is directly used to scan a fingerprint for enrollment. To use a USB fingerprint reader and a USB smart card writer for enrollment purpose, do not select this option.
- Get Wiegand String from BioEntry – Get Wiegand string from BioEntry reader. User ID can be extracted through the BioEntry reader from a reader which generates Wiegand string. The wiegand string is able to see Userinfo.
- User ID – Assign a new user ID. Cannot be duplicated.
- Name, Department, Title – Enter user information.
- Scan – Scan new fingerprint template. User should place his/her same finger twice all the times. If scanning is successful, scanned template is displayed.
- Delete – Delete saved fingerprint template.
- Test Matching – Scan new fingerprint and match it with the 1st template and the 2nd template by test.
- OK – Save the current user information into database of host PC.

3.5. Handling smartcard

- Read – Read the information of smartcard. Site key of smartcard should be

given correctly. (If it remains blank and then a user click 'OK' button, default primary key is automatically set)

A dialog box titled "Site Key" with a blue title bar and a close button (X) in the top right corner. It contains three text input fields: "Current Site Key", "Change Site Key" (preceded by an unchecked checkbox), and "Retype Site Key". At the bottom are "OK" and "Cancel" buttons.

- Write – Save the information displayed in the current form to smartcard. If site key has not been input from startup of program, site key can be changed and saved. If writing is stopped by external problems or some other factors in the writing process, the corresponding smartcard is not likely to be used any more - especially while changing site key.

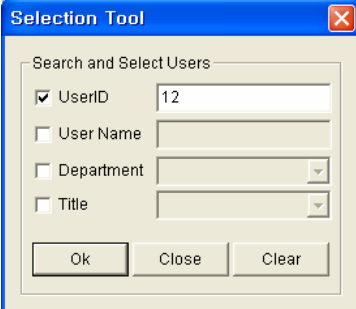
Warnings: Please pay your keen attention into writing the site key into a smart card.

- Format – Delete all information of smartcard. If site key has not been input from startup of program, it is possible to change site key.
- Security Level – When a user smart card is issued, Security Level can be selected in range of 3/10,000 to 1/100,000,000, or Bypass. If someone often fails to verify, adjust this option and issue a smart card again. When Bypass is selected, user can pass always with this smart card only without placing fingerprint.

3.6. Import User

Load the user list saved as CSV file format. You can recover user information except template data.

3.7. Selection Tool

A dialog box titled "Selection Tool" with a blue title bar and a close button (X) in the top right corner. It contains a section "Search and Select Users" with four checkboxes: "UserID" (checked), "User Name", "Department", and "Title". Each checkbox is followed by a text input field. The "UserID" field contains the value "12". At the bottom are "Ok", "Close", and "Clear" buttons.

This tool makes it possible to select users in the user list by a field and condition.

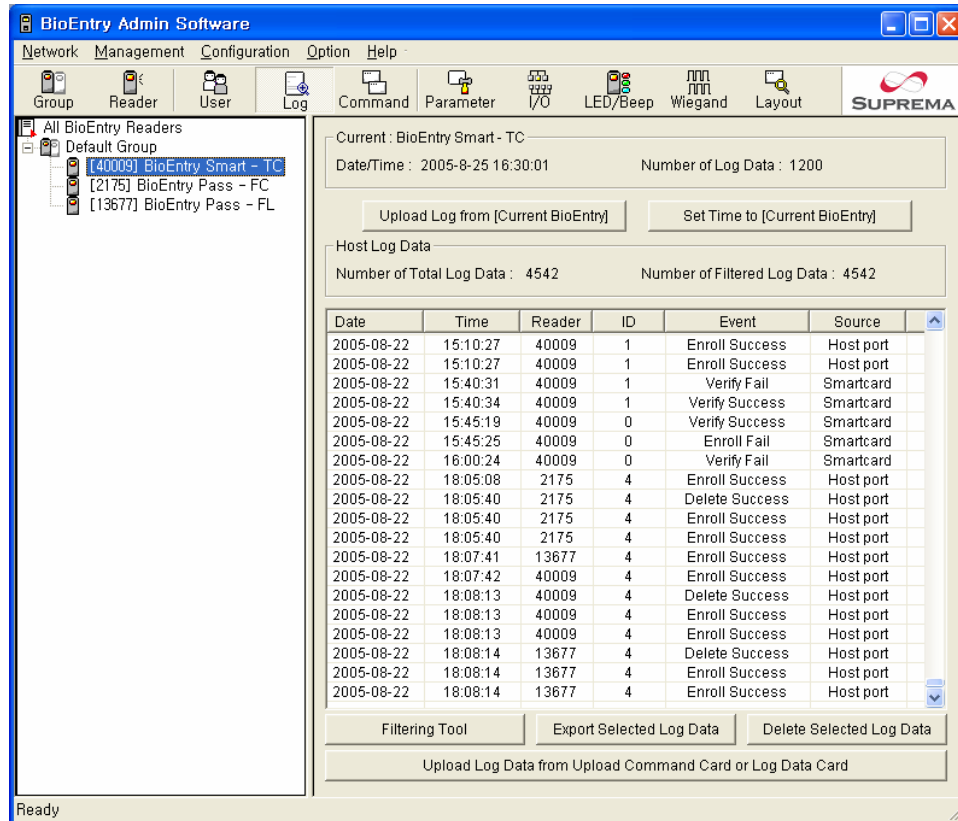
3.8. Export Selected User

Save the list of selected users as CSV file format. You can edit this file with Microsoft Office Excel or any text editor.

3.9. Delete Selected User

Delete the selected users from the database of host PC completely. Because user template cannot be uploaded from BioEntry to host PC, be careful to delete user data on host PC.

4. Log Management



4.1. Current

This section shows the number of log data and the time information saved in the selected BioEntry. No information is shown if group or All BioEntry Readers are selected.

4.2. Upload Log

Upload log data from all BioEntry readers, current group, or current BioEntry to host PC.

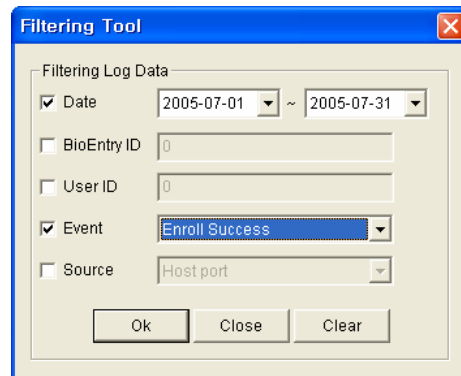
4.3. Set Time

Set the time of all BioEntry readers, current group, or current BioEntry as current time of host PC.

4.4. Host Log Data

This section shows the number of the log data saved in host PC.

4.5. Filtering Tool



This tool makes it possible to select log data by a field or condition separately.

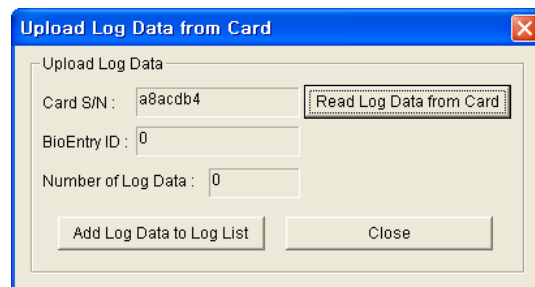
4.6. Export Selected Log Data

Save the selected log data as CSV File format.

4.7. Delete Selected Log Data

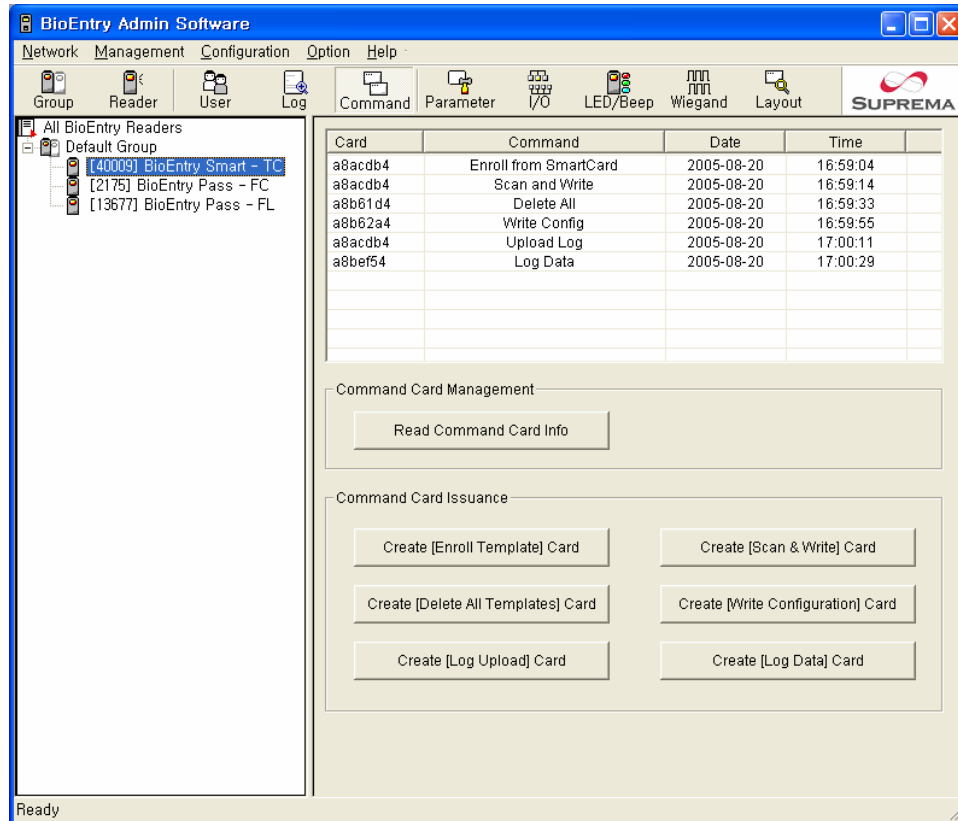
Delete the selected log data in host PC.

4.8. Upload Log Data from Command Card



Read Log Data Card from PC Reader. You can use only BioEntry – Smart. See section 10. Command card

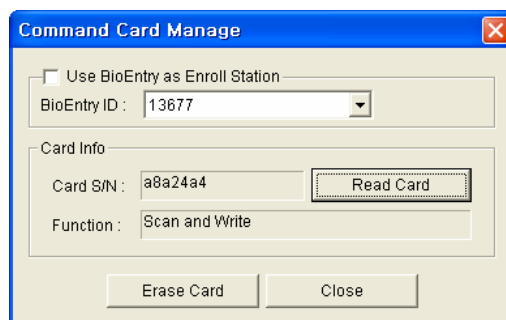
5. Command Card



5.1. Command Card List

This section shows and manages Command Card list. Command Card is a card which controls BioEntry without network.

5.2. Read Command Card



This can check the card issued. User can also erase the command card from command card list.

5.3. Issuance Command Card

- Issuance Enroll Template Card

Issuance: This function needs two smart cards. One card is a command card and the other is a user smart card which has User ID and templates. First, click this button. Then a popup window appears. User can issue a command card after scanning administrator's fingerprint in this popup window.

Usage: Place the command card to a BioEntry, BioEntry waits administrator fingerprint. If it is verified successfully, BioEntry wait a user smart card. Place the user smart card to BioEntry, BioEntry enrolls User ID and templates in this smart card.

- **Issuance Scan & Write Command Card**

Issuance: This function can issue a command card that scans and writes a user template to a smart card with User ID. The operation is the same as that of issuing Enroll Template Card.

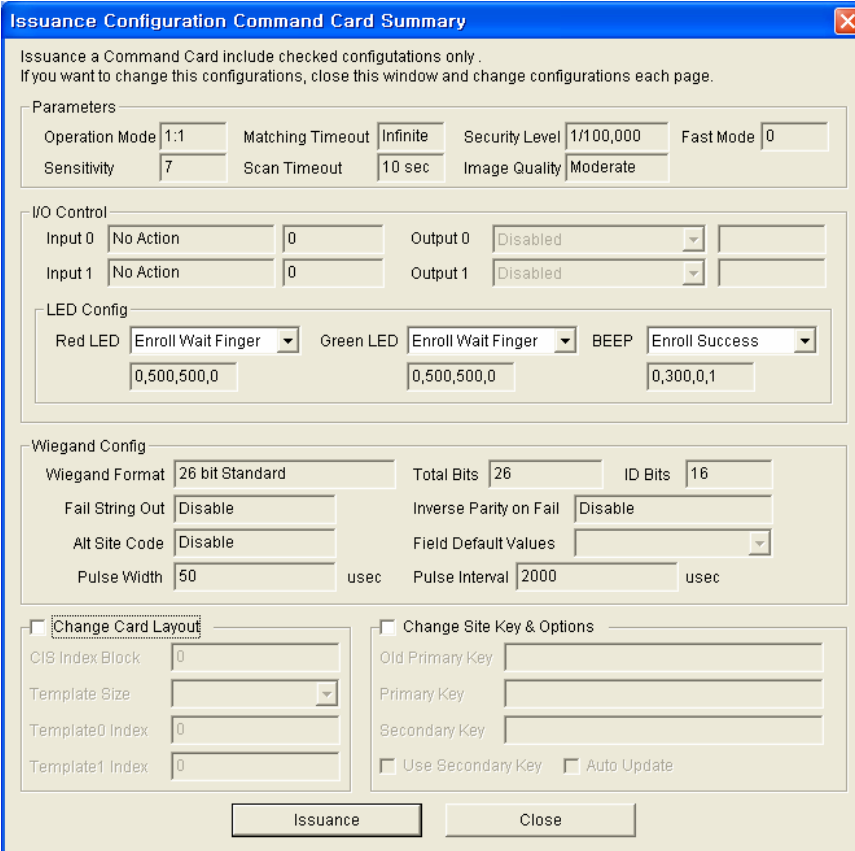
Usage: Place the command card to a BioEntry, BioEntry waits administrator's fingerprint. If verified successfully, BioEntry waits for scanning user's fingerprint 4 times. Then write these templates to a smart card.

- **Issuance Delete All Template Command Card**

Issuance: This function can issue a command card to delete all templates in BioEntry. The operation is the same as that of issuing Enroll Template Card.

Usage: Place the command card to BioEntry, BioEntry waits administrator's fingerprint. Scan administrator's fingerprint. Repeat it 2 times, then you can delete all templates in BioEntry.

- **Issuance Write Configuration Card**



Issuance Configuration Command Card Summary

Issuance a Command Card include checked configurations only .
If you want to change this configurations, close this window and change configurations each page.

Parameters

Operation Mode	1:1	Matching Timeout	Infinite	Security Level	1/100,000	Fast Mode	0
Sensitivity	7	Scan Timeout	10 sec	Image Quality	Moderate		

I/O Control

Input 0	No Action	0	Output 0	Disabled	
Input 1	No Action	0	Output 1	Disabled	

LED Config

Red LED	Enroll Wait Finger	Green LED	Enroll Wait Finger	BEEP	Enroll Success
	0,500,500,0		0,500,500,0		0,300,0,1

Wiegand Config

Wiegand Format	26 bit Standard	Total Bits	26	ID Bits	16
Fail String Out	Disable	Inverse Parity on Fail	Disable		
Alt Site Code	Disable	Field Default Values			
Pulse Width	50	usec	Pulse Interval	2000	usec

☐ **Change Card Layout**

CIS Index Block	0
Template Size	
Template0 Index	0
Template1 Index	0

☐ **Change Site Key & Options**

Old Primary Key	
Primary Key	
Secondary Key	

☐ Use Secondary Key ☐ Auto Update

Issuance **Close**

Issuance: This function can issue a command card to change BioEntry's system settings. This popup window is the summary configurations of current BioAdmin software. If you want to change the values of this summary window, close this popup window and change them in each section. To change smart card layout or site key & options, click each title to apply settings to a command card. Check each parameter in this popup window and click 'Issuance' button for issuance. Next operation is the same as that of issuing Enroll Template Card but it can need more smart card to write this configurations. Prepare one or more spare cards.

Usage: Place the command card to BioEntry. BioEntry waits administrator's fingerprint. Scan administrator's fingerprint. If it is verified successfully, place the next command card to BioEntry. All command cards are verified successfully and BioEntry's system settings are changed.

- **Issuance Upload Log Data Card**

Issuance: This function can issue a command card to upload log data from BioEntry. Just click 'Create [Upload Log] Card' button and click 'Issue' in popup

window, Issuance is end. To upload log data from the BioEntry to smart card, you need more Log Data Card's.

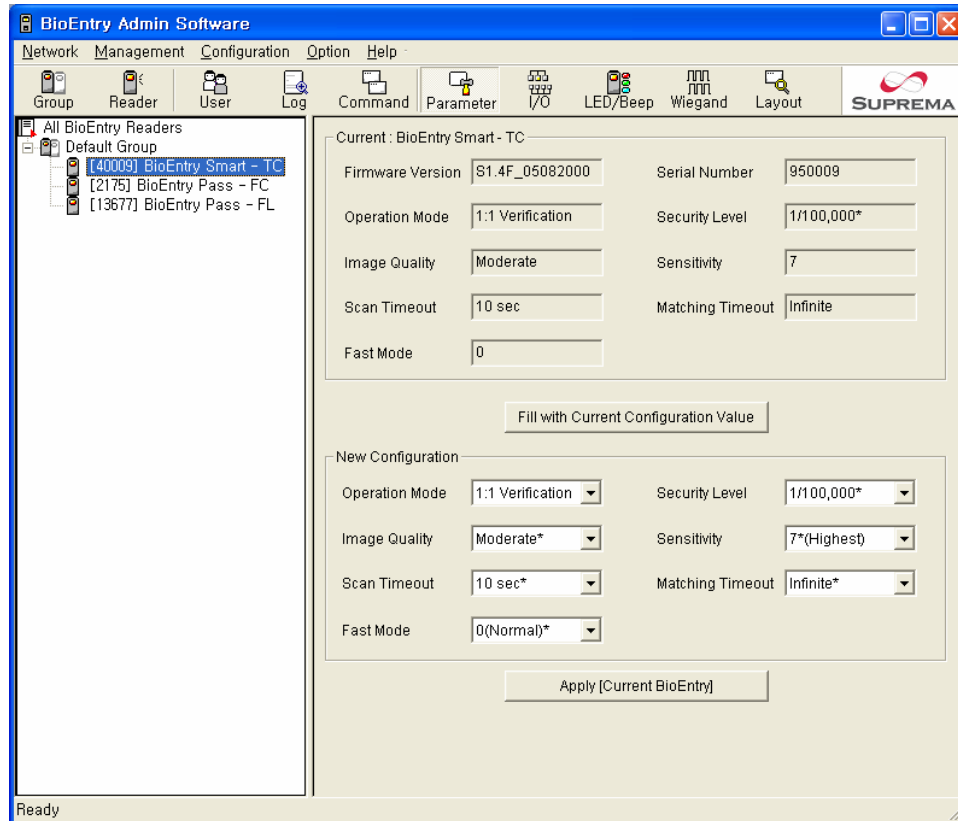
Usage: Place the command card to BioEntry, The BioEntry starts uploading log data to a command card. If BioEntry has more log data, it waits a log data card. See next.

- Issuance Log Data Card

Issuance: This function can issue a command card to upload log data. The operation of issuance is same as that of issuing Upload Log Data Card.

Usage: This command card can be used only after using Upload Log Data Card.

6. Parameter Configuration



6.1. Current Configuration

This shows current configuration value of the selected BioEntry.

6.2. Fill with Current Configuration Value

Fill new configuration value with current configuration value of the selected BioEntry.

6.3. Apply

Apply new configuration value to all BioEntry readers, current group, or current BioEntry.

6.4. Operation Mode

- 1:1 Verification – 1:1 verification mode using smartcard or Wiegand input.
- 1:N Identification – 1:N identification mode using free scan.
- Both – Use both 1:1 verification and 1:N identification mode.

6.5. Security Level

Security level specifies FAR(False Acceptance Ratio). If it is set to 1/100,000, it

means that the probability of accepting false fingerprints is 1/100,000. Since FAR and FRR(False Rejection Ration) is in inverse proportion to each other, FRR will increase with higher security levels

6.6. Image Quality

When a fingerprint is scanned, the module will check if the quality of the image is adequate for further processing. Image quality parameter specifies the strictness of this quality check.

6.7. Sensitivity

Specifies sensor sensitivity to detect a finger. On high sensitivity, the module will accept the finger input more easily. In other hand, by decreasing the sensitivity, the input fingerprint image will be more stabilized. In case of optical models, sensitivity to sunlight is also alleviated by decreasing sensitivity parameter.

6.8. Scan Timeout

Timeout period for user input. If users do not make his/her finger scanned, place smartcard, or input Wiegand, during this period, error will be returned.

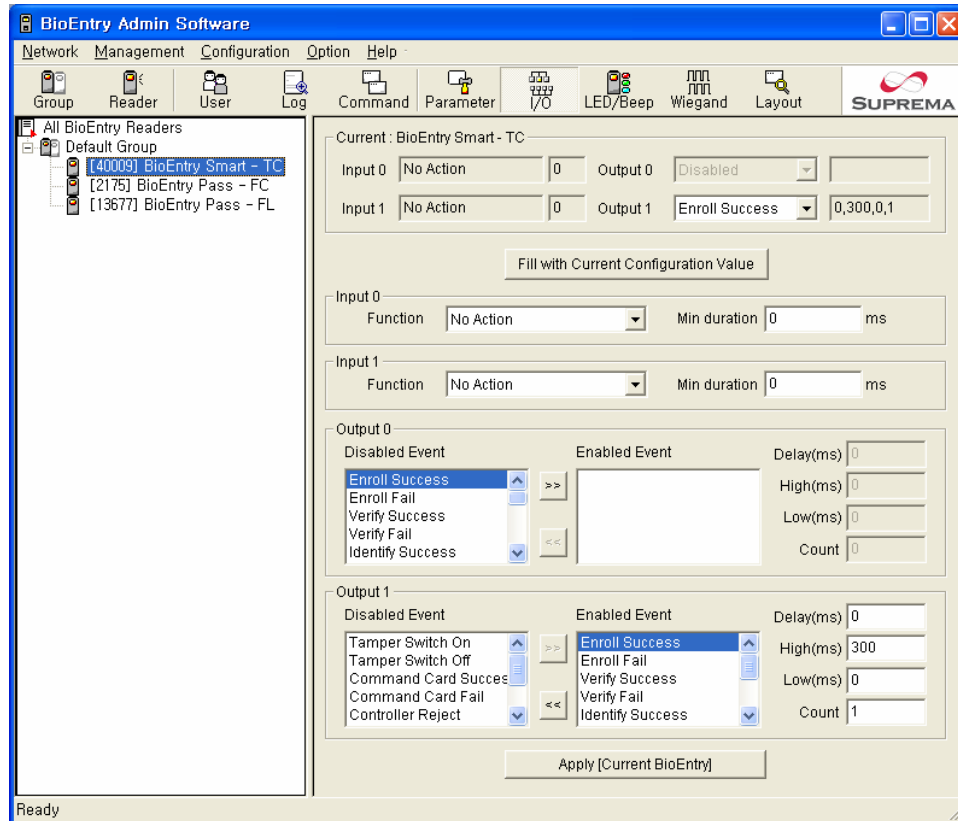
6.9. Matching Timeout

Timeout period for 1:N matching. If identification process is not finished until this period, error will be returned

6.10. Fast Mode

When more than hundreds of templates are stored in BioEntry, the matching time for 1:N identification can be very long. Fast Mode parameter can be used to shorten the 1:N matching time with little degradation of authentication performance. The security level – FAR – is not affected by this parameter, but the FRR can be a bit higher than normal mode. In typical cases, Fast Mode 1 as 2 ~ 3 times faster than Normal mode. And Fast Mode 5 is 6 ~ 7 times faster than Normal mode.

7. I/O Configuration



7.1. Current Configuration

This section shows the current configuration value of I/O Port of the selected BioEntry.

7.2. Fill with Current Configuration Value

Fill new configuration value with current configuration value of selected BioEntry.

7.3. Apply

Apply new configuration value to all BioEntry readers, current group, or current BioEntry.

7.4. Input port setting

Change the function of input port like number 0 and 1.

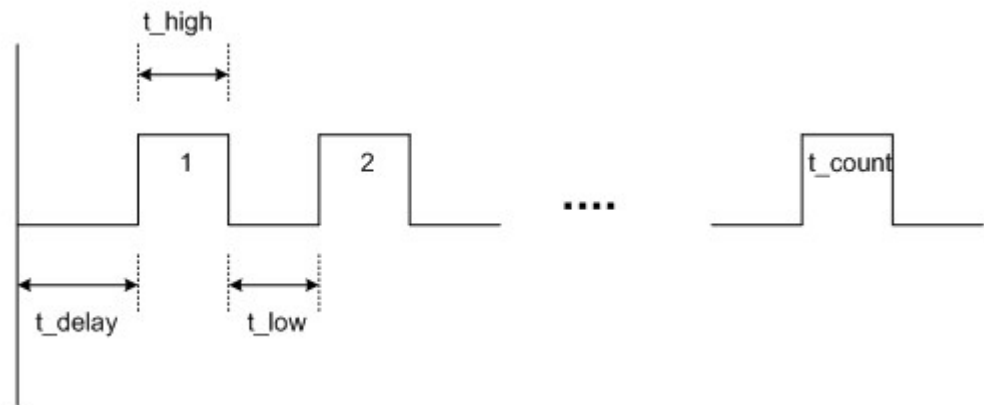
- Min Duration – Set the minimum duration of input pulse.

7.5. Output port setting

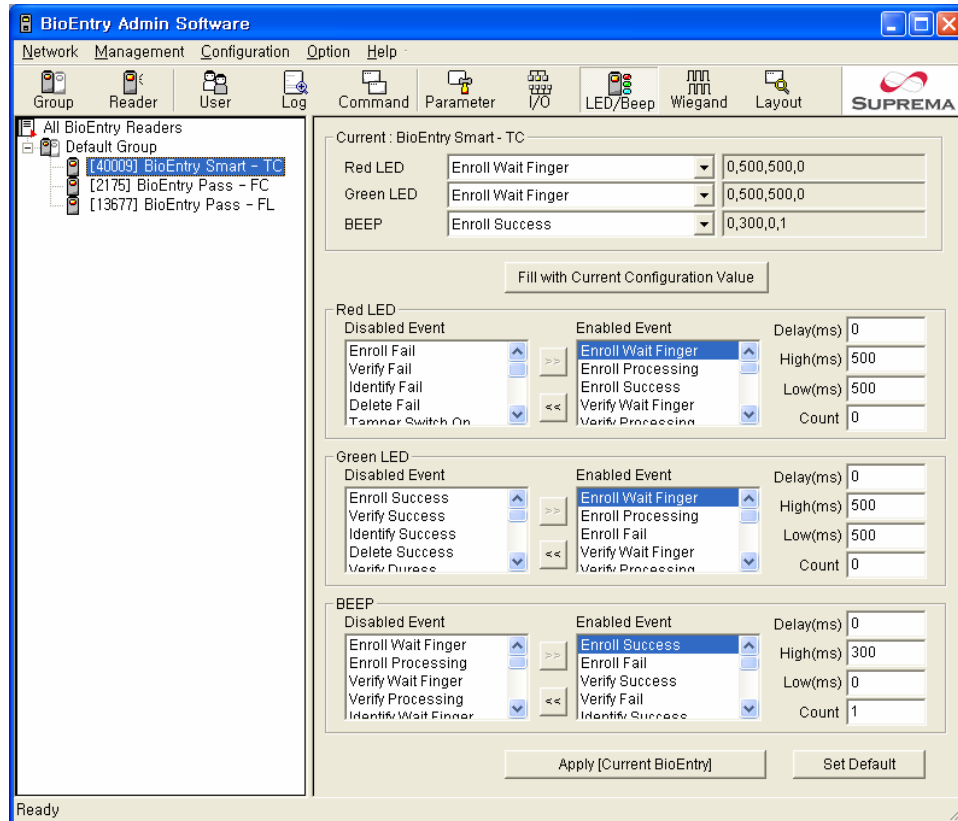
Change the function of the output port like number 0 and 1.

- Enabled Events – Multiple functions can be selected.

- The output pattern for each enabled function can be set.
- This figure shows meaning of output event parameters. Also LED/Beep Events.



8. LED/Beep Control



8.1. Current Configuration

This section shows the current configuration value of LED and Beep Event of the selected BioEntry.

8.2. Fill with Current Configuration Value

Fill new configuration values with current configuration values of selected BioEntry.

8.3. Apply

Apply new configuration values to all BioEntry's, current group, or current BioEntry.

8.4. Red, Green LED setting

Change the event of the red and green LED.

- Enabled Events – Multiple events can be selected.
- The LED pattern for each enabled function can be set.

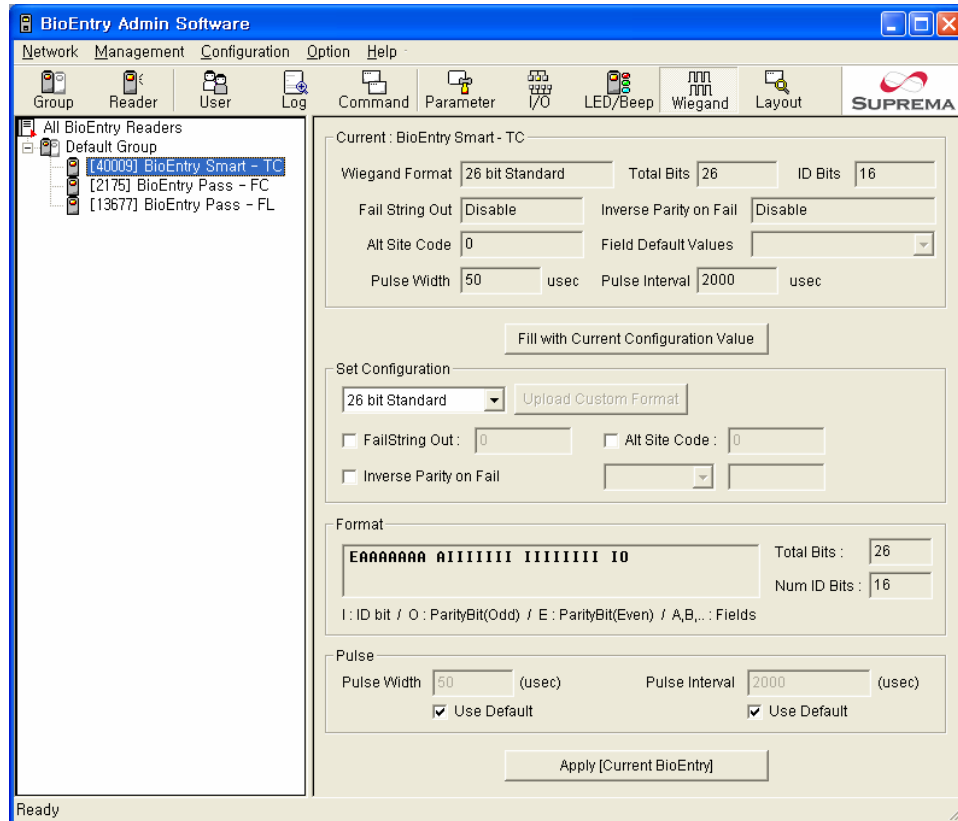
8.5. Beep setting

Change the event of the Beep.

- Enabled Events – Multiple events can be selected.

- The Beep pattern for each enabled function can be set.

9. Wiegand Configuration



9.1. Current Configuration

This section shows the current Wiegand configuration value of the selected BioEntry.

9.2. Fill with Current Configuration Value

Fill new configuration value with current configuration value of the selected BioEntry.

9.3. Apply

Apply new configuration value to all BioEntry readers, current group, or current BioEntry.

9.4. Set Configuration

Change the new Wiegand configuration value.

- Upload Custom Format – Set Wiegand configuration value from the formatted file.

9.5. Format

This part shows the simple information of the Wiegand format.

- Format – Shows the format of Wiegand string bitwise.
- Total Bits – The total bit number in Wiegand String
- Num ID Bits – The bit number relative to ID field in Wiegand String.

9.6. Pulse

Change the values of pulse width and pulse interval.

- Pulse Width – Change the values directly or set them as default.
- Pulse Interval – Change the values directly or set them as default.

9.7. Wiegand Format File

When a user selects Pass-through Format or Custom Format, Wiegand format configuration file can be edited directly.

- 26 bit standard

The 26 bit standard format is most widely used and consists of 8 bit site code and 16 bit ID. Users can set an alternative site code and enable advanced options.

- Pass Through format

Pass Through format is used when only the format of ID field is known. When Wiegand input string is detected, the module extracts ID bits and starts verification with the ID. If the verification succeeds, the module outputs the Wiegand input string as unchanged. Parity check and advanced options are ignored in this format. By definition, Pass Through format is only useful when the matching is initiated by Wiegand input. If the matching is initiated by Packet Protocol or GPIO input, the bits other than ID field are set to 0.

The definition data for Pass Through format is as follows;

Field	Byte	Description
Total bits	1	1~64
Number of ID fields	1	In most cases, it will be 1. However, if ID bits are composed of several fields, it would be larger than 1.
ID field 0 start bit	1	Start bit index of ID field 0
ID field 0 length	1	Number of ID field 0 bits
...		
ID field N start bit	1	Start bit index of ID field N
ID field N length	1	Number of ID N bits

For example, assume that 32 bit pass through format is composed as follows;

XIIIIII IIIIIIX XXXIIII IIIIIIX (left most bit is 0th bit, BIT0)

I: Id field, X: Unknown field

The definition data would be,

Total Bits	Num of ID fields	ID field 0 start index	ID field 0 Length	ID field 1 start index	ID field 1 length
32	2	1	14	19	12

- Example of Wiegand configuration file from the definition data (Pass-Through Format)

```
# '#' : Description ('#' means annotation.)
# field=value (Basic form : field = value)
#
# format_type : type of wiegand string format
#
#           1 : 26 bit Standard Format
#           2 : Pass-through Definition File
#           3 : Custom Definition File

format_type = 2 (Pass-through Format)
total_bits = 32 (The length of Wiegand string is 32 byte.)

num_of_fields= 2 (The total number of the fields is 2)

field0_start = 1 (the starting bit index of field1. The bit index starts from number 0.)
field0_length = 14 (the length of field0)

field1_start = 19 (the starting bit index of field1)
field1_length = 12 (the length of field1)
```

- Custom format

When users know all the information of a Wiegand format, Custom format can be defined. When Wiegand input string is detected, the module checks the parity bits first. If all the parity bits are correct, the module extracts ID bits and starts verification with the ID. Users can also set alternative values of each field and enable advanced options such as Fail ID. If the verification succeeds, the module outputs a Wiegand string. The output string may be different from the input string according to the alternative values and advanced options. The definition data of Custom format is as follows;

Field		Byte	Description
Total Bits		1	1 ~ 64
Number of fields		1	1 ~ 16
Field 0	Start bit index	1	Start bit index of the field
	Length	1	Number of bits: 1 ~ 32
...			
Field N	Start bit index	1	Start bit index of the field
	Length	1	Number of bits: 1 ~ 32
Number of parity bits		1	1 ~ 8
Parity 0	Type	1	0: Even, 1: Odd
	Bit position	1	Bit index of the parity bit
	Bit mask	8	Bit mask for identifying the bits which are include in calculating the parity
...			
Parity N	Type	1	0: Even, 1: Odd
	Bit position	1	Bit index of the parity bit
	Bit Mask	8	Bit mask
Bit Mask for ID field		2	Bit mask for identifying the fields which are part of ID

For example, assume that 44 bit custom format is composed as follows;

EIIIIII AAAAAAAAA AAAAAAAAA IIIIIIB BBBB BBBB BBBO

(left most bit is 0th bit, BIT0)

E: Even parity for BIT1 ~ BIT22 / O: Odd parity for BIT23 ~ BIT42

I: ID bits(Field 0 and Field 2), A: Field 1, B: Field 3

The field definition data would be,

Field		Value
Total Bits		44
Number of fields		4
Field 0	Start bit index	1
	Length	7
Field 1	Start bit index	8
	Length	16
Field 2	Start bit index	24
	Length	7
Field 3	Start bit index	31
	Length	12
Number of parity bits		2
Parity 0	Type	0: Even
	Bit position	0
	Bit mask	0x7FFFFE: Bit 1 ~ Bit 22
Parity 1	Type	1: Odd
	Bit position	43
	Bit mask	0x07FFFF800000: Bit 23 ~ Bit 42
Bit mask for ID field		05: Field 0 and Field 2

- Example of Wiegand configuration file from the definition data (Custom Format)

```
# '#' : Description ('#' means annotation.)
# field=value (Basic form : field = value)
#
# format_type : type of wiegand string format
#
#                               1 : 26 bit Standard Format
#                               2 : Pass-through Definition File
#                               3 : Custom Definition File
format_type = 3 (Pass-Through Format)
total_bits = 44 (The length of Wiegand string is 39 byte.)

num_of_fields = 4 (The total number of the fields is 2)

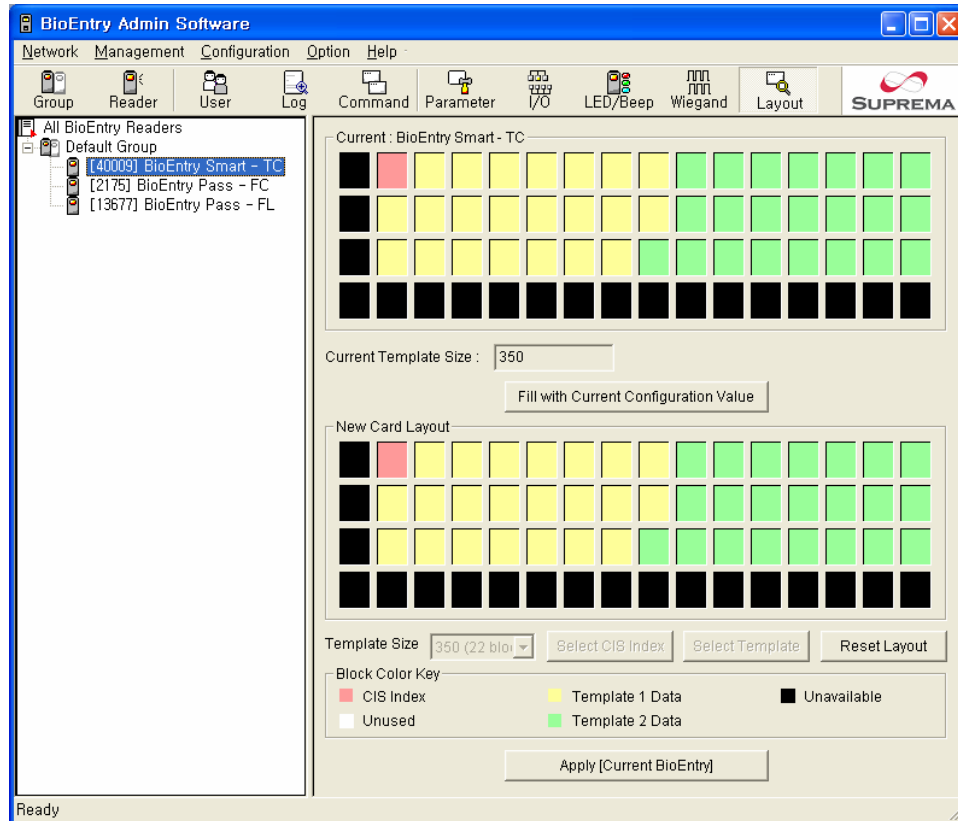
field0_start = 1 (the starting bit index of the first field. The bit index starts from number 0.)
field0_length = 7 (the length of the first field)
field1_start = 8 (the starting bit index of the second field)
field1_length = 16 (the length of the second field)
field2_start = 24 (the starting bit index of the third field)
field2_length = 7 (the length of the third field)
field3_start = 31 (the starting bit index of the 4th field)
field3_length = 12 (the length of the 4th field)
num_of_paritybits = 2 (the number of Parity bit)
parity0_type = 0 (the type of Parity0 Bit - 0:Even / 1:ODD)
parity0_position = 0 (the index of Parity0 Bit)
parity0_bitfield = 00000000007FFFFE (the bitfield of Parity0 Bit mask)
parity1_type = 1 (the type of Parity1 Bit)
parity1_position=43 (the index of Parity1 Bit)
parity1_bitfield = 000007FFFF800000 (the bit field of Parity1 Bit mask)
```

id_field_mask = 05 (the Mask to set the ID field among the Fields, "id_field_mask = 05" means field0 and field2 are ID field.)

It is not necessary to write annotation in Wiegand configuration file.

Recognize regardless of the order of each item. Exceptionally, the number of the field is recognized orderly. If field3_start is input as 1, actually the bit index of the third field is set to the position of the number 1 bit. The file should be text file format. Any file name is ok.

10. Smartcard Layout



10.1. Current Card Layout

This shows smartcard layout of the selected BioEntry.

- Current Template Size – Template size of the selected BioEntry.

10.2. Fill with Current Configuration Value

Fill new configuration value with current configuration value of the selected BioEntry.

10.3. Apply

Apply new configuration value to all BioEntry readers, current group, or current BioEntry.

10.4. New Card Layout

Change the layout of smartcard.

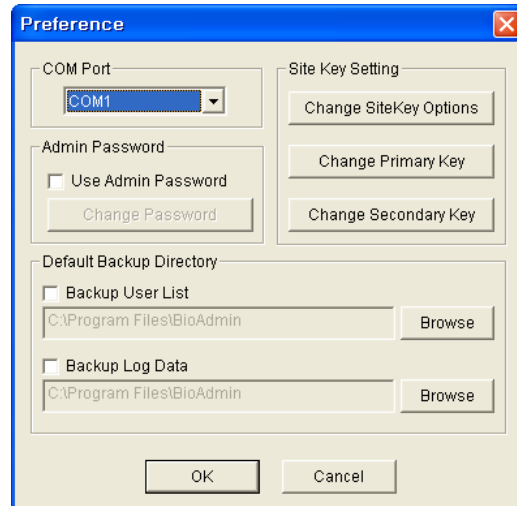
- Template Size – Set the size of template. The size of one block is 16 byte. Default value is 350 bytes.
- Select CIS Index – CIS index block can be positioned by clicking as you want to position. Because CIS index uses one block, any unused block can be

clicked.

- Select Template – The blocks for the first and the second templates can be chosen. If the start block of each template is clicked, the block of the corresponding template is set automatically, based on the size of template. If there is no remaining block as much as the template size, it cannot be clicked.
- Reset Layout – Initialize all the block unused. This makes all buttons returned to an activated state again.

Note: When you write to a smart card using PC Smart Card Reader, the New Card Layout is used. If the layout of BioEntry and layout of Smart Card are different, BioEntry cannot access a smart card.

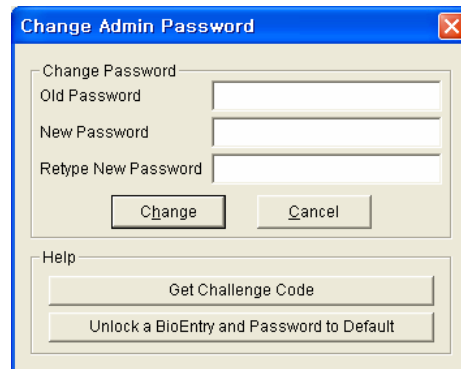
11. Preference



11.1. Com Port

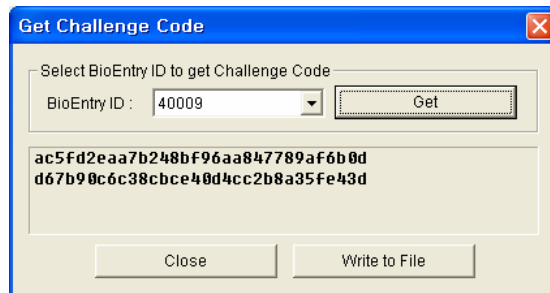
Select a port used for communication from COM1 to COM8.

11.2. Admin Password

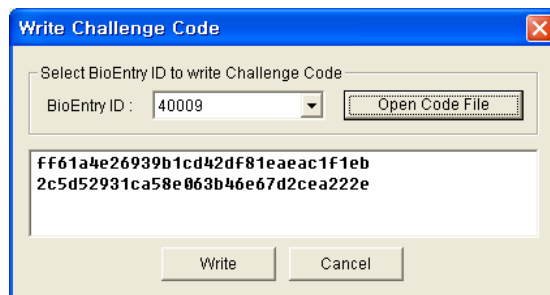


Change administrator password of all connected BioEntry's.

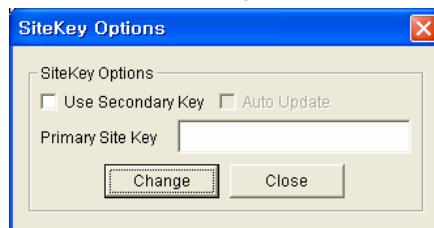
- Challenge Code is the key of Admin password which user forgot. When user gets the challenge code, BioEntry remembers this challenge code. Click 'Write to File' button and send this challenge code file to sales@supremainc.com.




- Suprema sends unlock code to user. Click 'Unlock a BioEntry and Password to Default' and select received file.



11.3. Site Key Setting



- Use Secondary Key - BioEntry readers use two site keys. If the site key of smart card is matched to one of these site keys, BioEntry can access the smart card. If you want to use 'Auto Update' function, this option should be turned on.
- Auto Update – If you need to update site key in all of smartcard, turn on this option. Assume that the primary site key is A, and the secondary site key is B. This option changes the site key of smart card to A, if user places the smart card, of which site key is A or B, at BioEntry.
- Changing site key – Change Primary Site Key / Secondary Key menu changes all connected BioEntry's. When primary site key, secondary site key, and site key options are changed, the old primary site key must be input.

A screenshot of a Windows-style dialog box titled "Change Primary Site Key". It has a blue title bar with a close button (X) in the top right corner. The dialog contains three text input fields: "Current Primary Key", "New Primary Key", and "Retype Primary Key". Below the fields are two buttons: "OK" and "Cancel".

Change Primary Site Key

Current Primary Key

New Primary Key

Retype Primary Key

OK Cancel

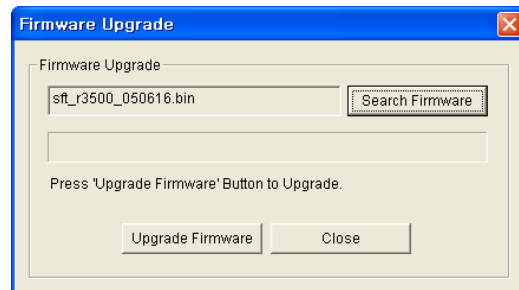
- Each site key can have an integer value from 0 to 281,474,976,710,655. If the input box of primary key remains blank, the default primary site key, 281,474,976,710,655, is input automatically.

Warnings: Please pay your keen attention to handling site key because lost site key can not be recovered.

11.4. Default Backup Directory

- Check and select any directory to save backup files.

12. Firmware Upgrade



12.1. Search Firmware & Upgrade

- Select a firmware file by clicking the Search Firmware button.
- Execute upgrade by clicking the Upgrade Firmware button.
- If BioEntry is turned off or reset in the process of upgrading, restoration may be impossible. If there is any problem in the process of upgrading, try to upgrade again in the state of BioEntry which is not reset.
- All BioEntry readers or group cannot be selected in the case of Firmware Upgrade. That is, upgrade can be possible after selecting only one BioEntry.

Contact Information

Suprema Inc.

DongCheon Bldg. 13-21 Yangjae-dong Seocho-gu Seoul 137-130 Korea

Tel: +82-2-571-9202

Fax: +82-2-571-9306

Website: <http://www.supremainc.com>

Sales inquires : sales@supremainc.com

Technical inquires : support@supremainc.com