BioEntry™ Operation Manual

BioEntry™ Smart / Pass

Ver. 2.0

SUPREMA

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

The 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 engines. 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 the 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 70 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 manage templates of respective BioEntry™, properly adjust relevant parameters, enroll or delete templates, etc. The purpose of this manual is to provide instructions to using BioEntry™ Smart and Pass and troubleshooting tips.

Contents

Revision History

Version	Date	Description
V1.0	2005.09.27	Created.
V1.1	2005.12.02	Incorporated the changes made by BioAdmin V1.1. Chapter 12. Site Key is added.
V2.0	2006.04.17	Incorporated the changes made by BioAdmin V2.0. Chapter 8. Access Control is added. Chapter 9. Monitoring is added.

1. Getting Started

This manual illustrates how to operate BioEntry™ Smart and Pass which are fingerprint access readers compliable to conventional physical access control systems. In general operations, BioEntry™ readers are connected to controllers via standard Wiegand interface and optionally connected to host PC through RS232, RS422 or RS485 network for advanced management. BioEntry™ Smart can be used without connecting to host PC since fingerprint templates are stored on user's smart card. For proper hardware connection, please refer to *BioEntry™ Installation Guide.*

There are two approaches in managing BioEntry™ readers:

- Using BioAdmin program which is the management software running on Windows based PC platforms. This manual is mainly focused on operating BioEntry™ readers using BioAdmin software.
- Integrating the management functionality into customer's application software using SDK which contains versatile API's to control the readers. For further information, please refer to *SFM SDK Reference Manual* and *UniFinger Engine SDK Reference Manual*.

This manual covers the following issues on operating BioEntry™ Smart and Pass.

1.1. Backgrounds

Introductive information on BioEntry™ readers and BioAdmin software is provided in Chapter 2. Backgrounds. This chapter will be helpful for users to understand the operation of BioEntry™ readers comprehensively.

1.2. Quick start

Quick start guide is presented in Chapter 3. Quick Start. By following operation examples presented in this Chapter step by step, users can understand basic operation flow of BioEntry™ readers more quickly.

1.3. Network setup

BioEntry™ can be connected through RS232/RS422/RS485 network line with host PC using BioAdmin software.

- To search all connected BioEntry™ readers through the selected COM port automatically, please refer to Chapter 4. Networking BioEntry™ readers.
- To divide multiple BioEntry™ readers into several groups, please refer to Chapter 4. Networking BioEntry™ readers.

1.4. Security setting

Security settings including smart card site key and administrator's password are also described in Chapter 11. Site Key and Chapter 12. Preference.

- To enhance security, BioAdmin software can lock BioEntry™ when the software is closed. If BioEntry™ is locked, BioAdmin software asks administrator's password when trying to unlock. If a wrong password is entered, BioEntry™ will remain locked. Execute 'Unlock All Readers' and enter a correct password to unlock BioEntry™. Please refer to Section 12.2. Automatic Locking and Password Management.
- For BioEntry™ Smart series, the site key of BioEntry™ must be changed at first and a user should remember it. Please refer to Chapter 11. Site Key.

User database of BioAdmin software includes user information and fingerprint templates. Detailed information to manage user database is described in Chapter 5. User Management.

- To add a new user into user database, please refer to Section 5.5. Add New User.
- For BioEntry™ Smart series, user fingerprint templates should be stored on a smart card. Please refer to Section 5.5.2. Issuing user's smart card.

1.5. Log management

BioAdmin software supports easy management of event log data stored on BioEntry™ readers.

1.6. Configuration of BioEntry™

BioAdmin software provides easy methods to configure BioEntry™ depending on the application circumstances.

- To change the system parameters such as operation mode, security level, and timeout, please refer to Chapter 6. Device Management. 오류! 참조 원본을 찾을 수 없습니다.
- To change the configuration of programmable I/O, please refer to Chapter 6. Device Management.
- To change the LED status and beep sound of BioEntry™, please refer to Chapter 6. Device Management.오류! 참조 원본을 찾을 수 없습니다.
- To change Wiegand format, please refer to Chapter 6. Device Management. 오류! 참조 원본을 찾을 수 없습니다.
- For BioEntry™ Smart series, if the layout of a smart card is different from the default layout, it should be configured before issuing a user smart card. To configure the layout of smart card, please refer to Chapter 7.5 Configure Card Layout. 오류! 참조 원본을 찾을 수 없습니다.

1.7. Configuration of BEACon™

BioAdmin software provides the menus to manage BEACon™ door controller.

- To change the Relay and Switch settings, refer to Chapter 6.7 BEACon™ Configuration. This chapter also shows the procedures to manage other configurations and password of BEACon™.

2. Backgrounds

This chapter provides introductive information on BioEntry™ readers and BioAdmin software including basic concepts, operation flow, and overview of the software.

2.1. Basic concepts

2.1.1. Fingerprint access reader

Fingerprint access reader is a device to authenticate the identity of each person using fingerprints. It can be easily integrated into access control system by connecting with access control panel through industry standard interface such as Wiegand interface. Since fingerprints contain biometric features which are unique for each person, fingerprint access reader can be substituted for existing access readers, such as barcode, magnetic card, keypad, or RF card readers, with high security and efficiency.

2.1.2. Fingerprint smart card reader

Fingerprint smart card reader is an advanced model of fingerprint access reader which improves security of the system by integrating smart card technology. Fingerprint data for each person is stored on user's smart card and the reader authenticates the user by comparing the stored fingerprint data in the smart card with the input fingerprint data.

2.1.3. Template

A template is the binary data representing the features of each fingerprint. The fingerprint image acquired from a fingerprint sensor is converted to a template, which is stored on the memory of the fingerprint access reader or on user's smart card. In authenticating a user, a new template is also generated and compared with the stored templates.

2.1.4. Enrollment

Enrollment is the process to store the fingerprint template with user information.

Through enrollment process, new users are entered into the application system.

2.1.5. Verification

Verification is the process of authenticating an input fingerprint with the fingerprint of the specified user. On BioEntry™ Smart, a user places smart card containing personal fingerprint template and user information. Then, the reader carries out verification process by scanning an input fingerprint. On BioEntry™ Pass, verification process can be implemented by connecting external Wiegand reader, such as RF card reader, which provides the current user ID.

2.1.6. Identification

Identification is the process of searching a matched fingerprint among the stored fingerprints on the reader. BioEntry™ Pass basically operates in identification mode, which requires no additional input except the placement of a finger.

2.1.7. User database

User database is the entity of user information including user ID, user name, fingerprint templates, and so on. BioEntry™ Admin software is based on the central management of user database. That is, the user database is created, updated, and stored on the host PC. Then, it is selectively distributed to the BioEntry™ readers connected on the network using synchronization techniques.

2.1.8. Transfer

Transfer to Device is used to transmit the user database of the host PC to BioEntry™ readers. The user information such as User ID, templates, access group, and security level is transferred by this process.

Detailed operations are as follows.

- Enroll new users on BioEntry™
- Replace inconsistent templates on BioEntry™
- Delete templates of unknown users or de-selected users on BioEntry™

Transfer from Device is used to upload the user formation from BioEntry™ to the database of host PC. The user information such as User ID, Template Number, Number of Access Group, and Security Level can be uploaded by this process.

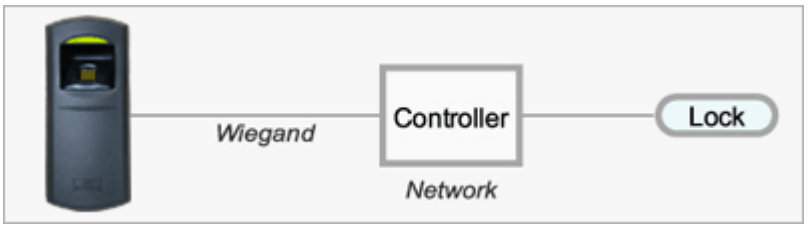
2.1.9. Site key for smartcard

Site key is a password for smart card to ensure that an authorized card should be used for a specific installation. 48 bit key is used in BioEntry™ Smart allowing 0 to 281374976710655 (0xFFFFFFFFFFFF). For proper operation, the same key should be configured on BioEntry™ Smart and user's smart card.

2.2. Operation configurations

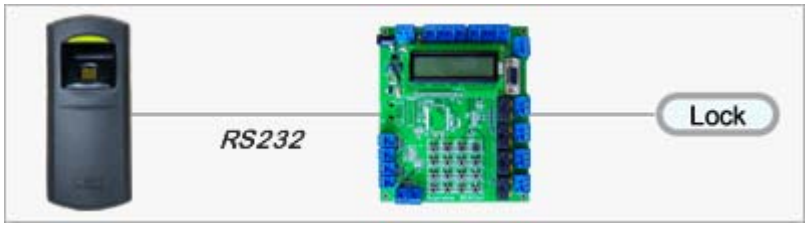
2.2.1. Standalone configuration

In simple applications where a controller for one door is required, standalone configuration can be built up using BioEntry™ Smart or BioEntry™ Pass. In this application, BioEntry™ is connected to controller through Wiegand interface and the door is controlled by the controller.



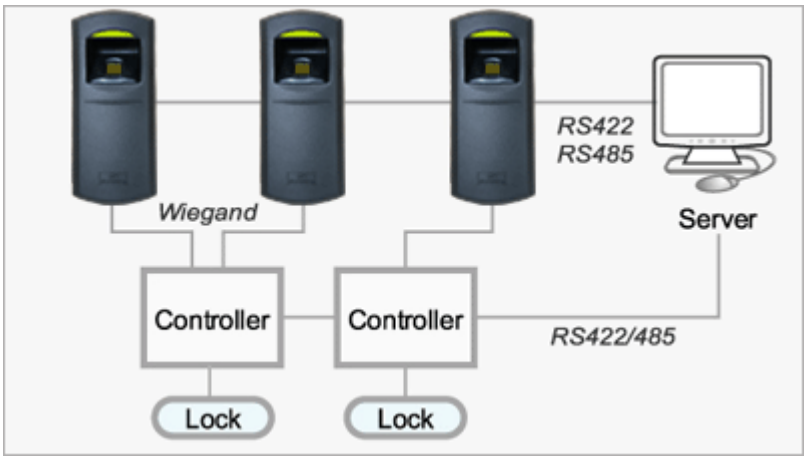
BioEntry™ Smart is operated with user's smart card, which is issued on host PC or by using the command card. For BioEntry™ Pass, it is required to enroll the user's template through the Aux. port.

When Suprema's BEACon™ is used as the door controller, BioEntry™ is connected to BEACon™ through RS-232 interface and the door is controlled by BEACon™.



2.2.2. Network configuration

In complex applications where the network setup is required to control multiple readers, BioEntry™ readers are connected to the network through RS232/422/485 interface. Readers are also connected to the controller via Wiegand interface to control the doors.

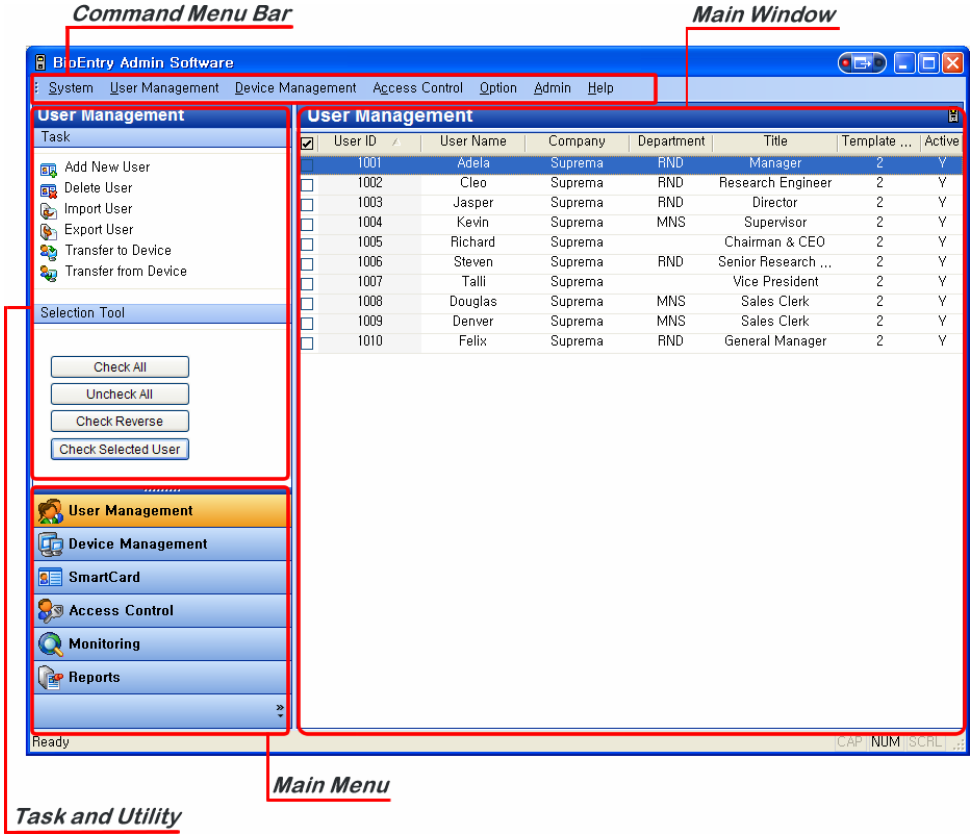


Users are enrolled in BioEntry™ Pass through the network and various management and configuration of the readers are processed through the network.

Moreover, when Suprema's BEACon™ is used as the door controller, devices can be connected through Ethernet interface with the built-in Ethernet converter of BEACon™.

2.3. Composition of BioAdmin

BioAdmin Software is composed of 4 elements, command menu bar, main menu, task and utilities, and main window.



2.3.1. Command menu bar

Command menu bar contains command items supported by Admin software, which are grouped into 6 categories:

- **System** : Load old data, Back up/Restore Database, and Lock/Unlock BioEntry readers.
- **User Management** : Add new user, Company management, Department Management, Title Management, and Sep up Custom Fields.
- **Device Management** : Search/Add new device, Set time, Upgrade firmware, Get/Set challenge code, and Site Key Setting.
- **Access Control** : Time code definition, Holiday Setting, Time Zone Setting, Door Zone Setting, and Access Group Setting.
- **Options** : System options and miscellaneous commands.

- **Admin** : Add/ Change/ Delete the Admin User of the BioAdmin™ software

2.3.2. Main menu

Major command menus can be accessed by buttons on the left pane, such as user management, device management, smart card, access control, monitoring or report.

2.3.3. Task and utilities

Task window shows sub-menus for the selected main menu

Utility window shows the User selection tool, Device tree, and Log filtering tool.

2.3.4. Main window

On each command menu, relevant information is updated on the main window. Main window contains the following information and controls:

- Retrieved information from currently selected reader
- Information stored on host PC, such as user database or log data
- Controls to manage or to configure the information

3. Quick Start

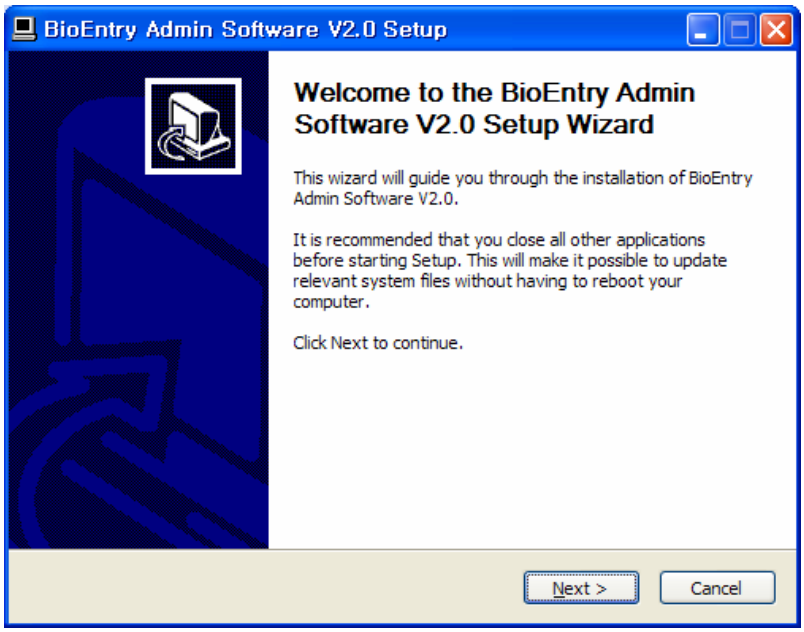
This chapter describes basic procedure to operate BioEntry™ readers integrated with external systems.

3.1. Installation of software

Suprema provides management software for BioEntry™ readers named by BioAdmin. Software installation is automatically processed by the setup program (BioAdmin Setup*.exe).

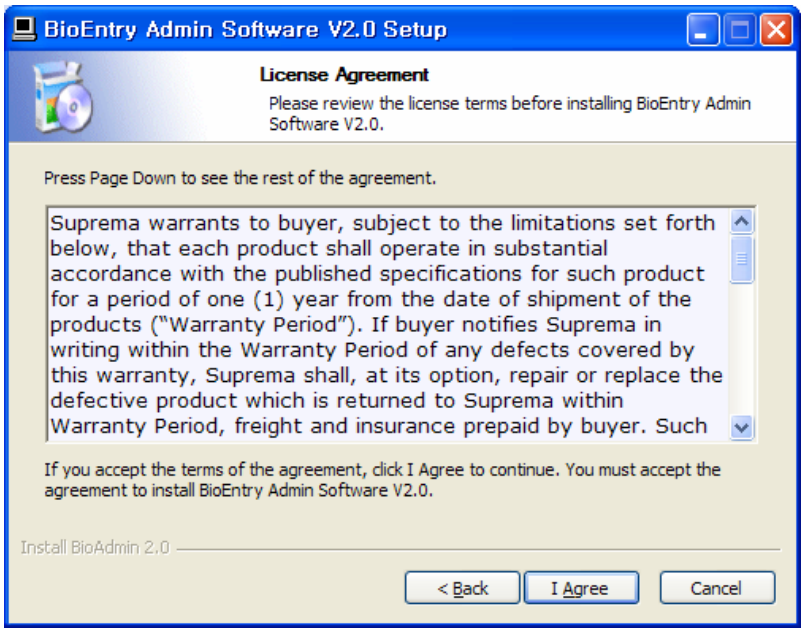
3.1.1. Step 1: Execute the setup program

By executing the setup program, the introductive message appears on the window. Press **Next** button to continue installation.



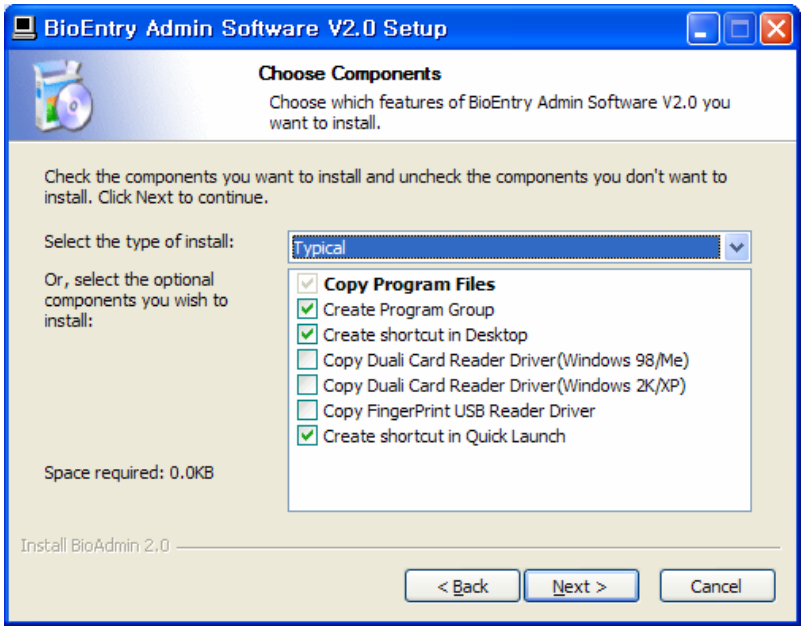
3.1.2. Step 2: License agreement

Read carefully the license agreement and press **Agree** button to accept the license agreement.



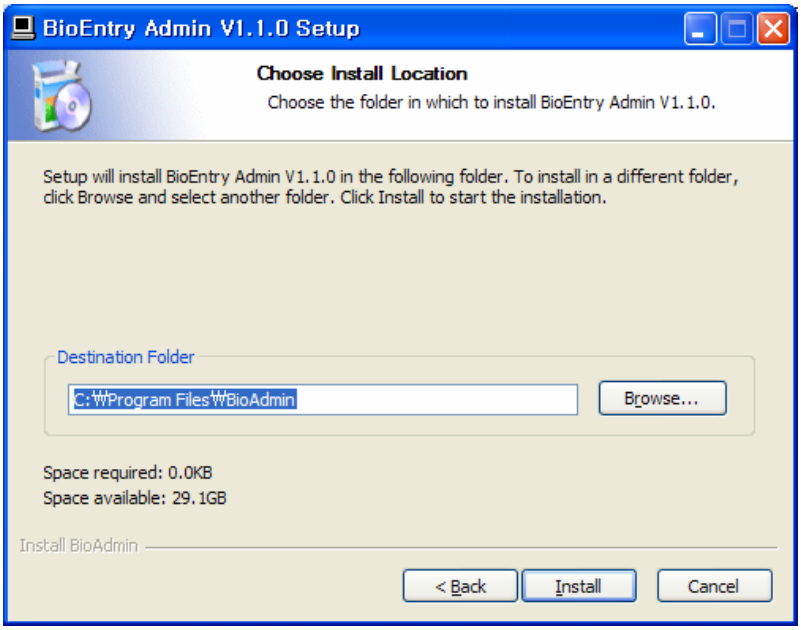
3.1.3. Step 3: Selection of components

Choose the components to install. If a smart card reader or USB scanner is used on the host PC, check **Copy Duali Card Reader Driver** or **Copy Fingerprint USB Reader Driver**, respectively. Then, press **Next** button.



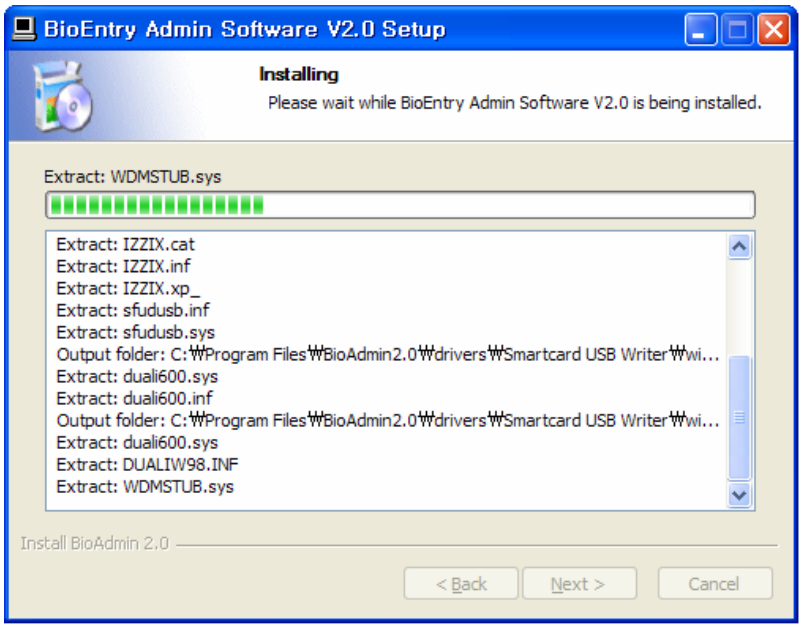
3.1.4. Step 4: Choose install location

Specify the folder where BioAdmin will be installed. Then, press **Install** button.



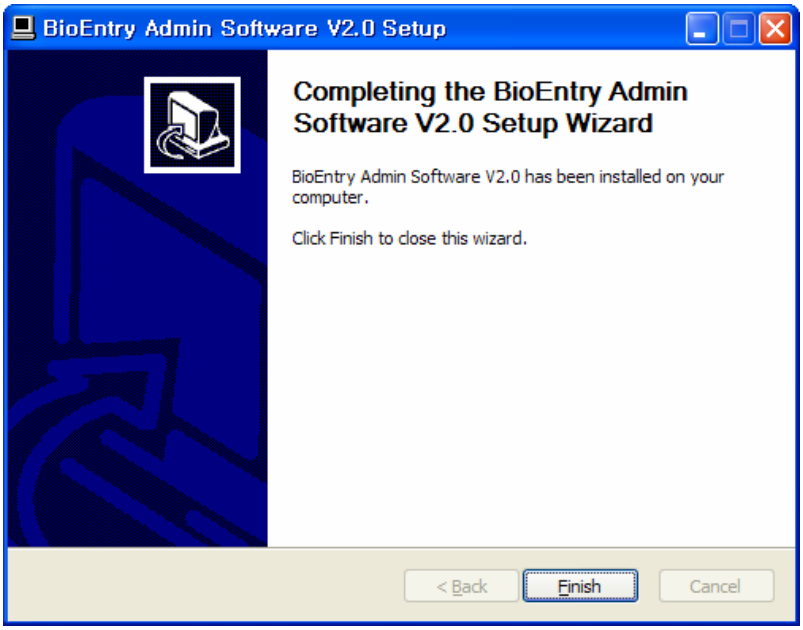
3.1.5. Step 5: Copying files

Install BioAdmin in the selected location.



3.1.6. Step 6: Installation complete

Finally, selected components are installed on the PC.

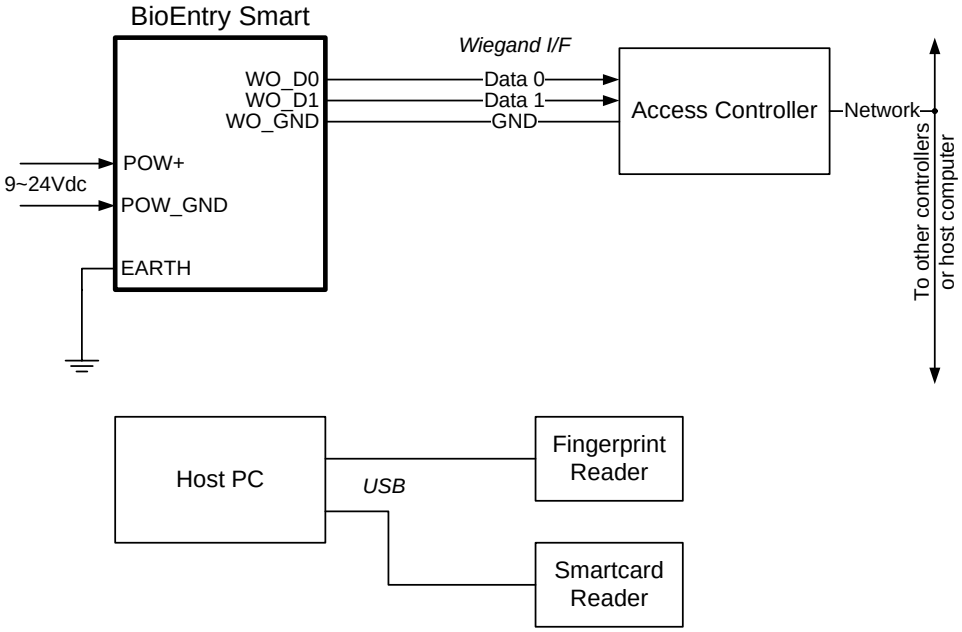


3.2. Quick start with BioEntry™ Smart

This section describes the basic procedures to operate BioEntry™ Smart using a USB fingerprint scanner and smart card reader as its enrollment device.

3.2.1. Step 1: Hardware installation

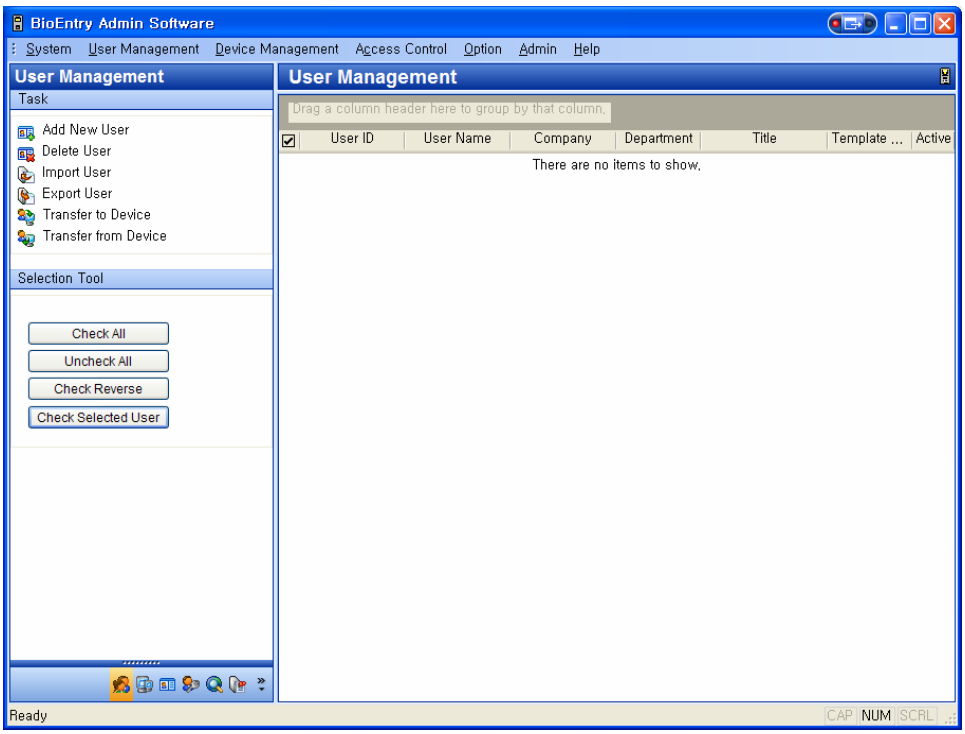
In this hardware configuration, the reader is not connected to the host PC, but to an external controller via Wiegand interface. It is assumed that the controller supports the standard 26 bit Wiegand format as default on BioEntry™ reader. Connect the reader with the controller as shown on the following configuration.



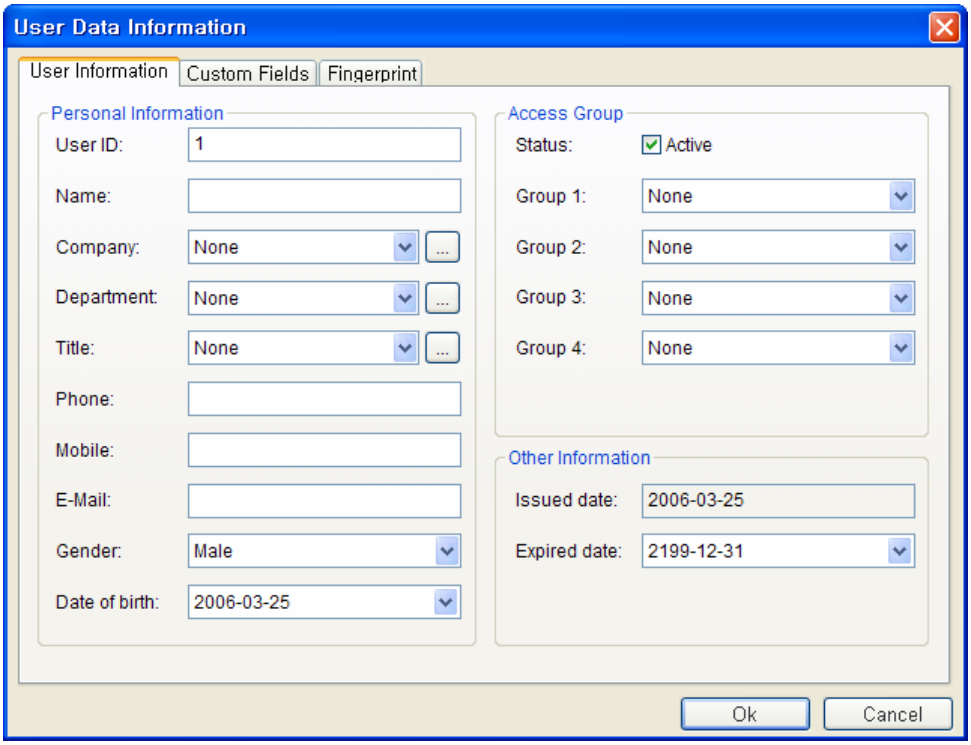
For more details on the installation, refer to the BioEntry™ Installation Guide or BEACon™ Operation Manual.

3.2.2. Step 2: Registration of user

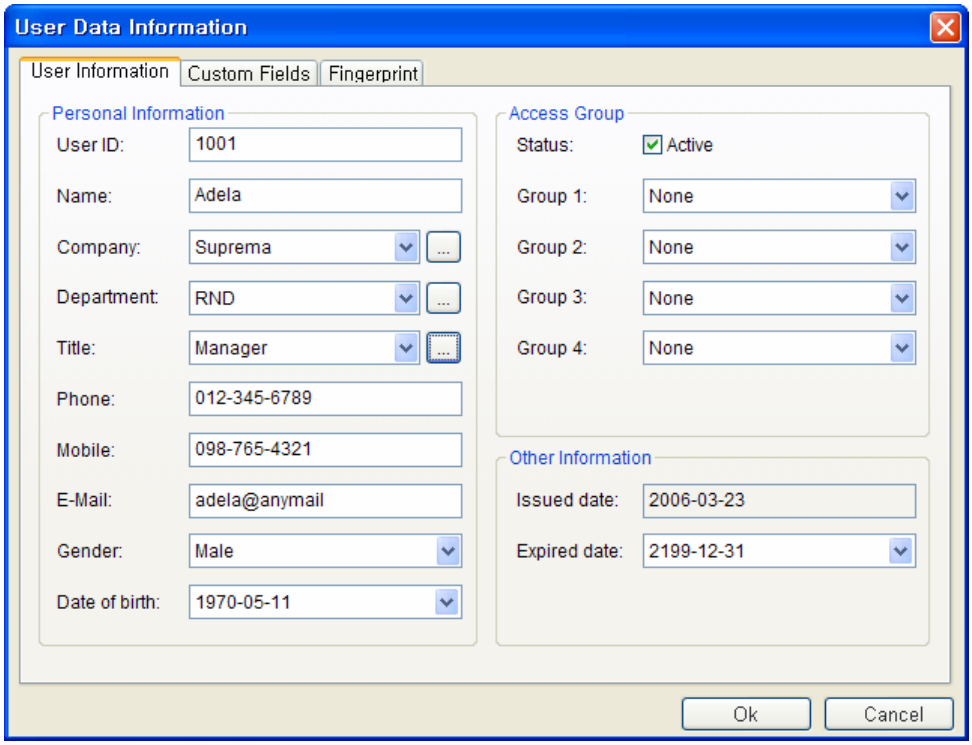
- Run BioAdmin software.
- Enter Login ID and password. By factory default, the initial Login ID is "**admin**" and the password is blank.
- Select **User Management** on the main menu, then the user management page appears on the main window.



- Select the **Add New User** menu on the task window, then the pop-up window appears

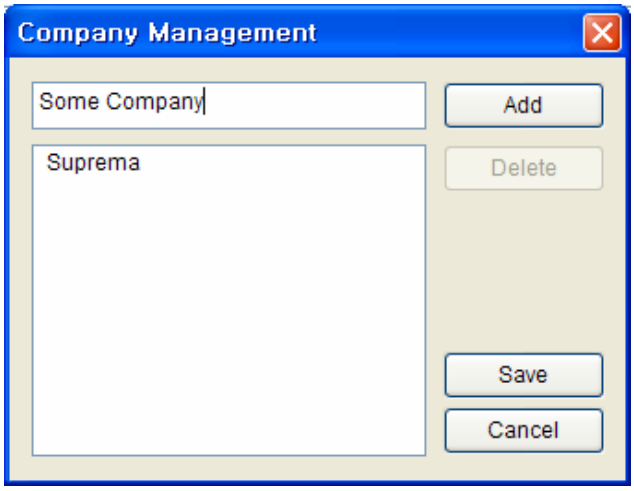


- Enter the **user information** on the User Information tab.



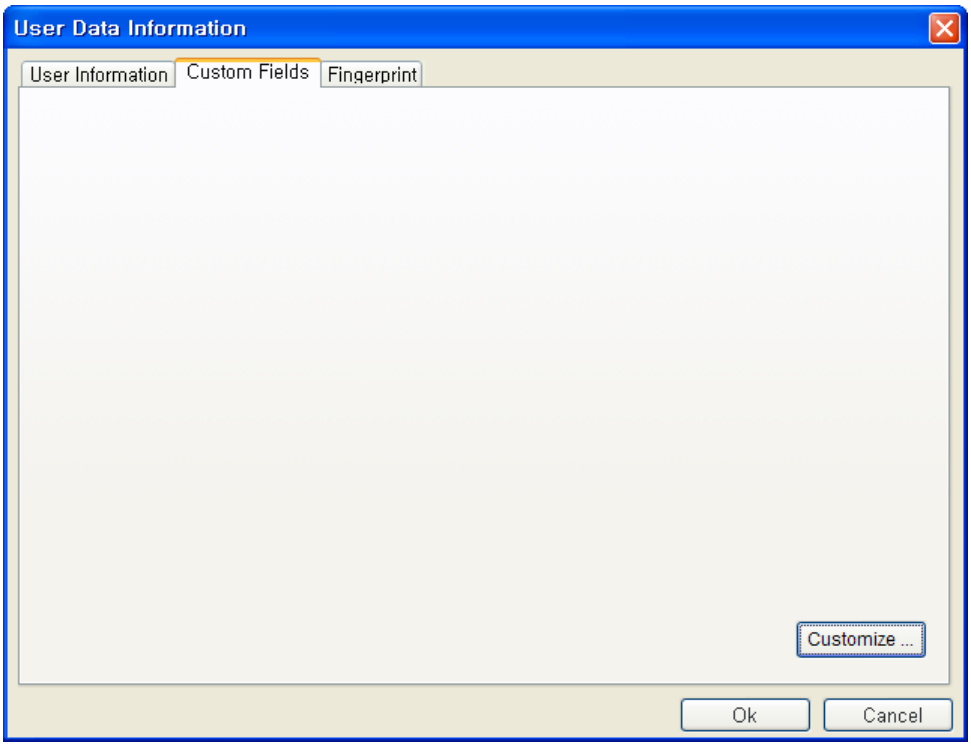
- Especially, you can select the Company, Department, and Title on the drag down menu.
- To add new Company, Department, or Title information, press button. After entering the required information, press **Add** button.

  Press **Save** button to save the added information.

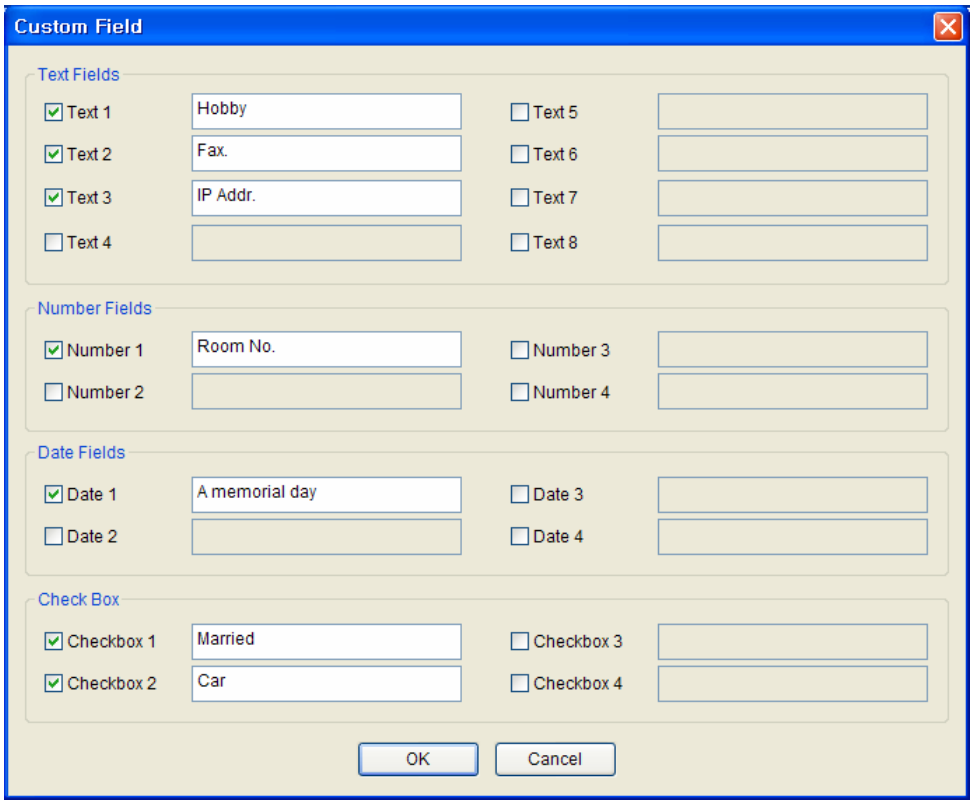


- In addition to the basic user information, you can add **Custom Fields** to the user information. If you do not need these custom fields, just skip the custom fields setting.

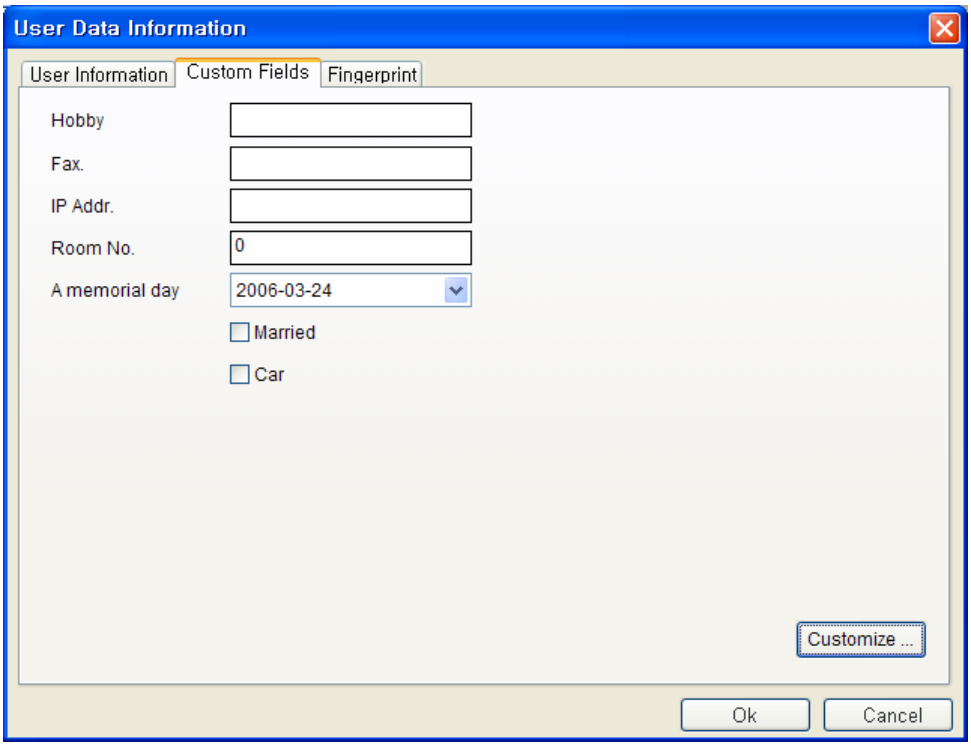
  To set up the custom fields, press **Custom Fields** tab.



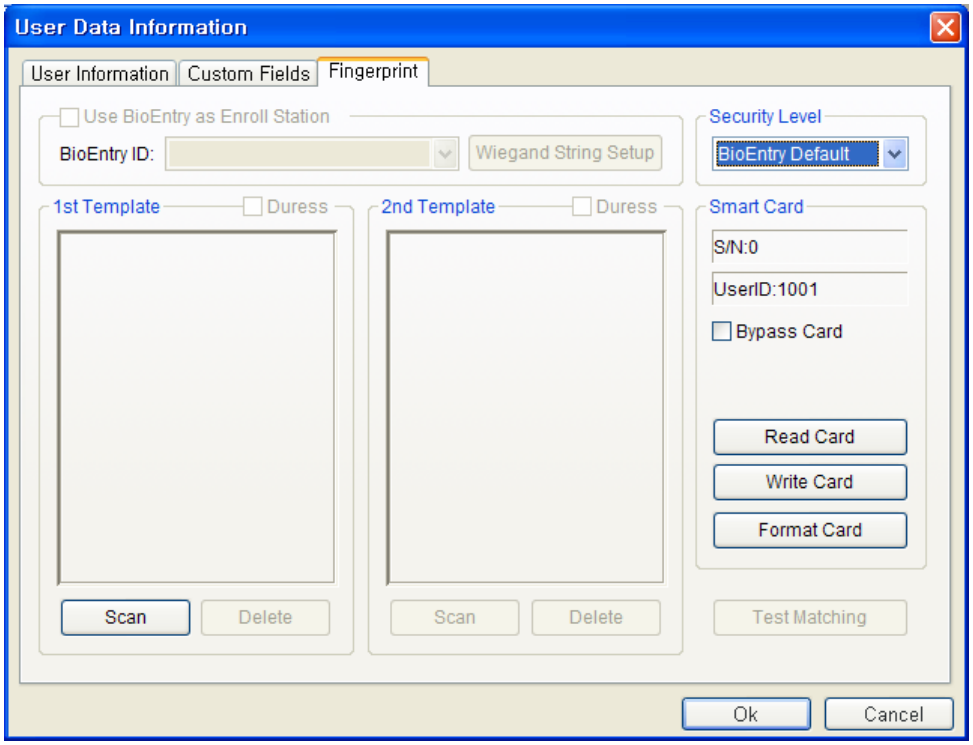
- Click the **Customize...** button.
- Check on the required Fields and enter the user information for those selected fields.



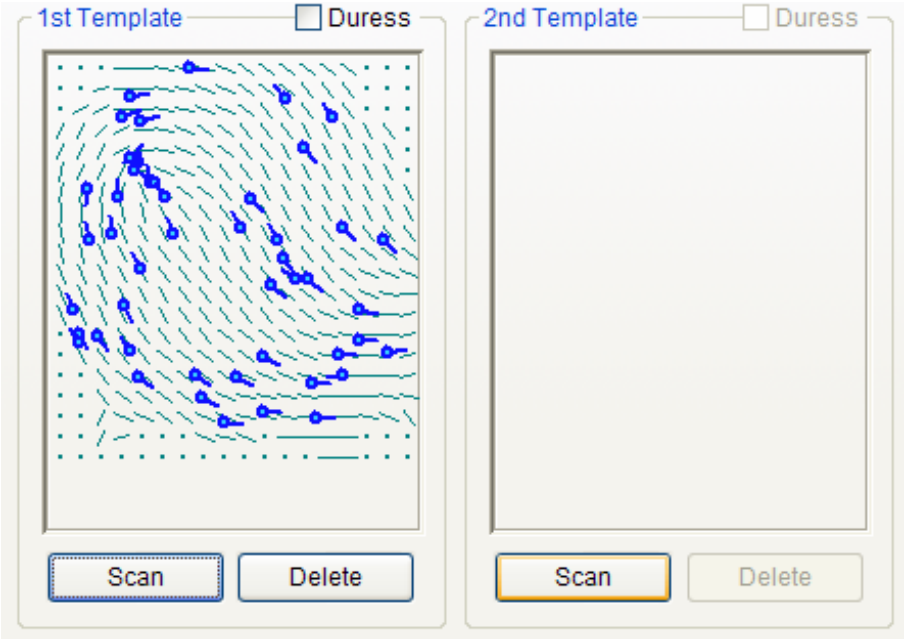
- After entering the user information, press the **OK** button.
- After filling out the custom fields, the following pop-up window will appear. On this window, you can see the details of your selected custom fields. Press **OK** button to save these custom fields.



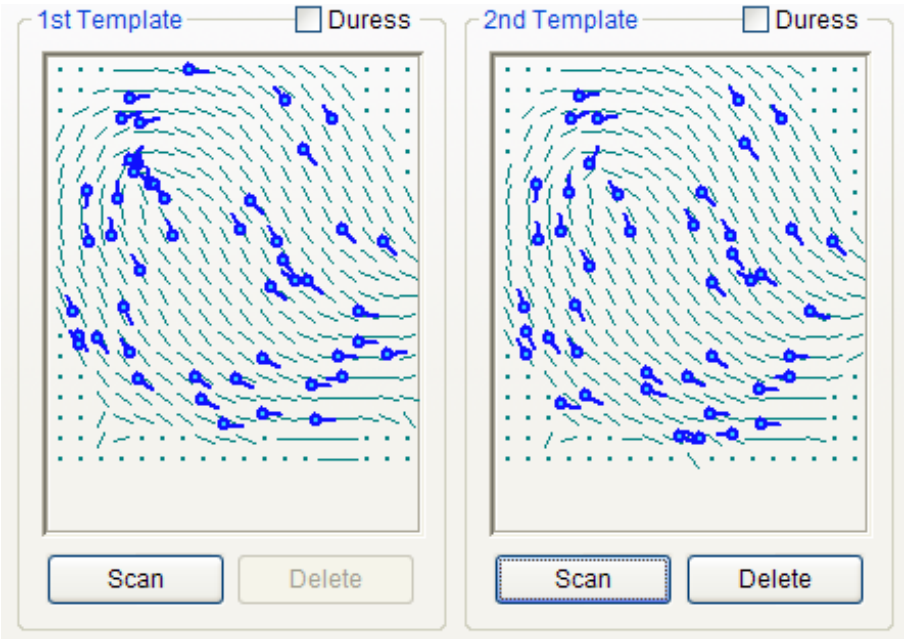
- After entering the user information, press the **Fingerprint** tab to enroll user's fingerprint templates.



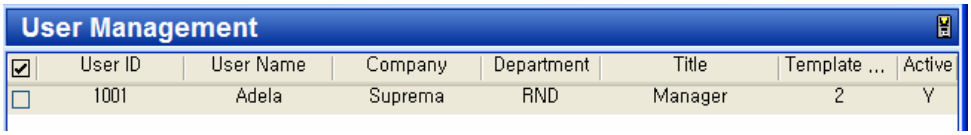
- Acquire first template by pressing the **Scan** button followed by touching finger on the USB fingerprint scanner twice.



- Acquire second template similarly to the acquisition of first template.

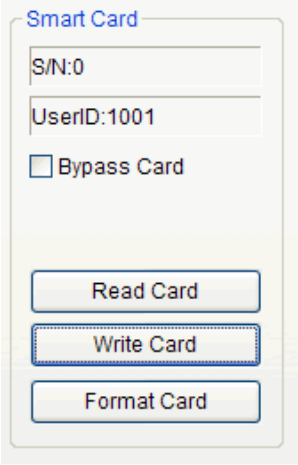


- Press the **OK** button to complete the registration process. Then, you can see the information of the registered user on the user list window. It means that user's information is added to the database on host PC.

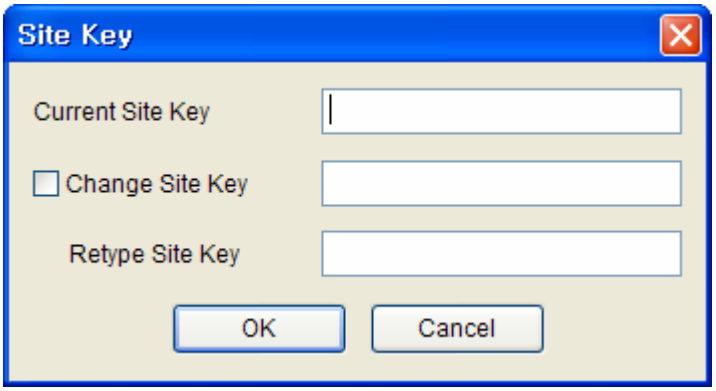


3.2.3. Step 3: Issuing user's smart card

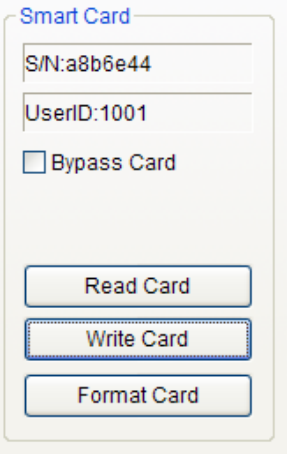
- Double click the registered user on the user list. Then, the user information window appears showing the registered information of the user.
- Click **Fingerprint** tab on user information window.
- Place a smart card on PC USB smart card reader and press **Write** button.



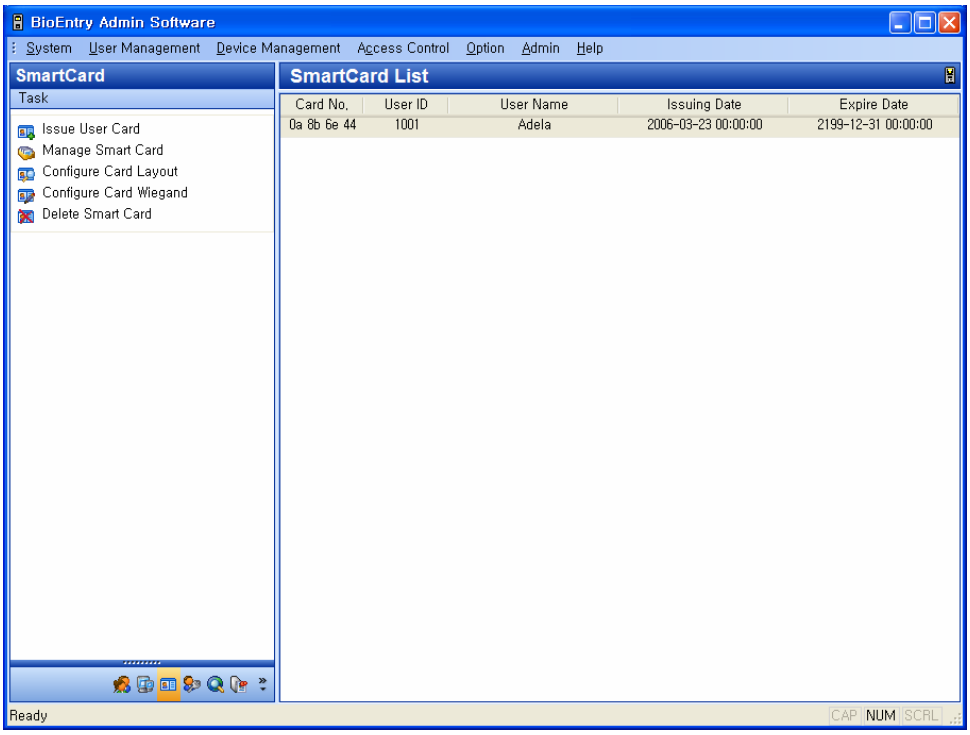
- At first trial, site key management window appears. If the key input remains blank, factory default key is used. So, just press **OK** button to complete issuing process if the site key was not changed from factory setting.



- On the user list window, you can see the serial number of the smart card.



- Select the **Smart Card** menu. Then you can see smart card is added on the list.



3.2.4. Step 4: Register user ID on the external controller

It is required that the issued user ID is also registered to the controller to grant access when the Wiegand string for the user is received.

If you are using Suprema's BEACon™ controller, you can just skip this additional registration to the controller.

3.2.5. Step 5: Test verification

Procedure to test verification using the user's smart card is as follows :

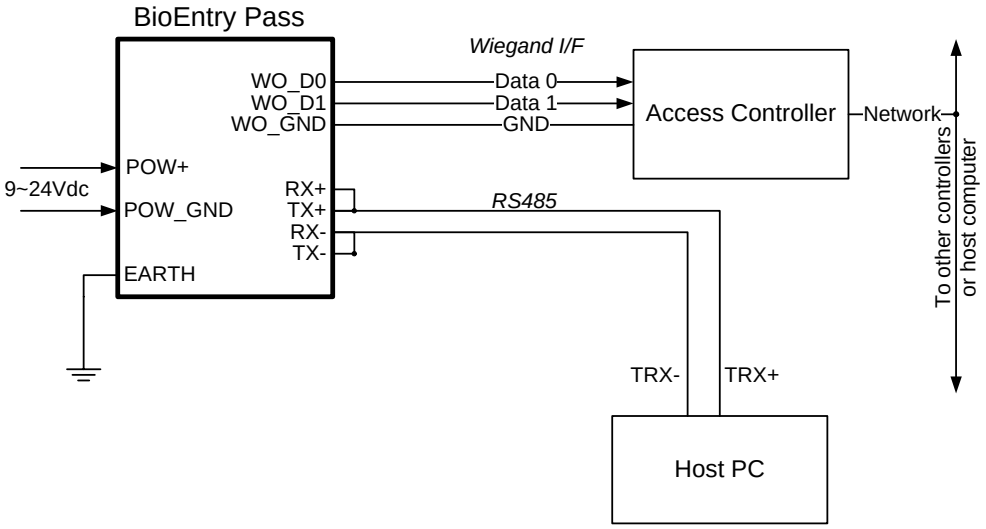
- First, place the user's smart card in front of the reader below the sensor. Then, amber LED blinks rapidly indicating that the reader is waiting for finger scan for verification.
- Place a finger on the sensor. If the user is successfully verified steady green LED appears with one beep sound. Otherwise, red LED appears with 3 beep sounds.
- On successful verification, the Wiegand string is also sent to the controller, which can be checked by operation of relay on the controller.

3.3. Quick start with BioEntry™ Pass

This section describes the basic procedures to operate BioEntry™ Pass without a PC reader.

3.3.1. Step 1: Hardware installation

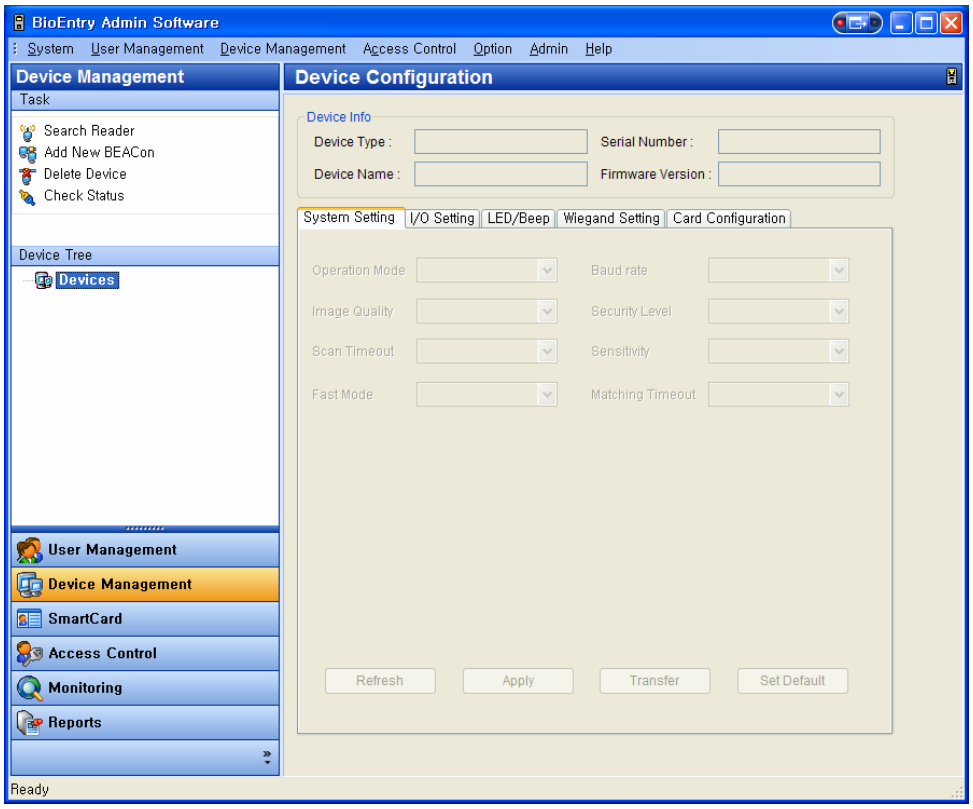
In this configuration, the reader is connected to an external controller via Wiegand interface as well as to the host PC through RS485 interface. It is assumed that the controller supports the standard 26 bit Wiegand format as default of BioEntry™ reader.



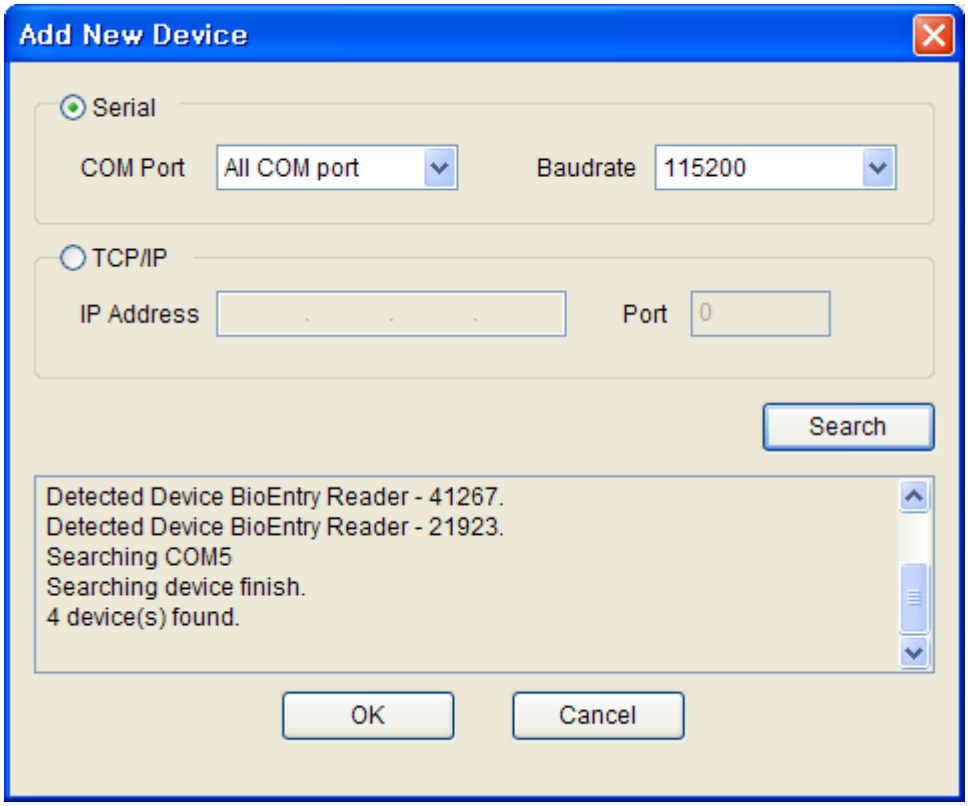
For more details on the installation, refer to the BioEntry™ Installation Guide or BEACon™ Operation Manual.

3.3.2. Step 2: Search Reader

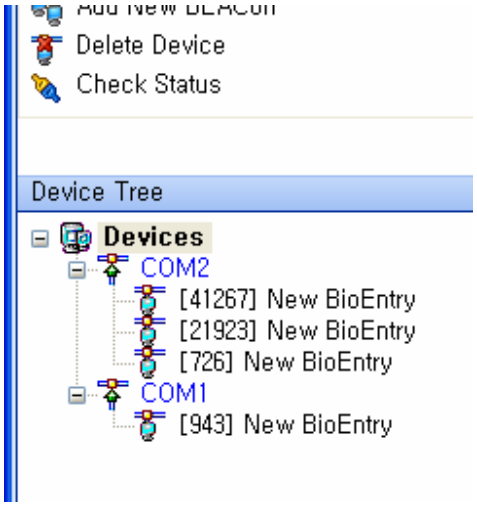
- Run BioAdmin software.
- Enter Login ID and password. By factory default, the initial Login ID is "**admin**" and the password is blank
- Select **Device Management** on the Main menu, then device management page will appear on the main window.



- Select the **Search Reader** menu and click the **Search** button. After searching BioEntry™ reader, press the **Ok** button.



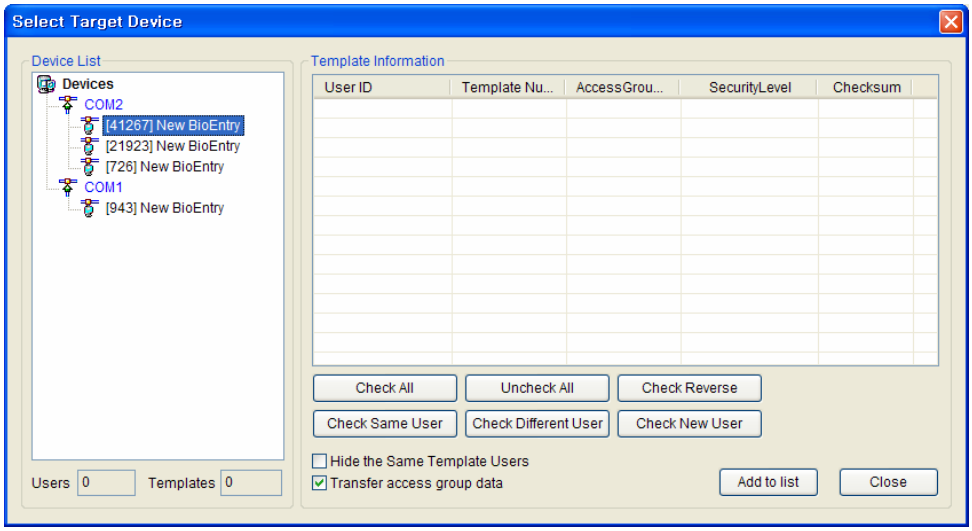
- If the readers are connected properly, new reader ID appears on the Device Tree window.



- Select the **User Management** button on the main menu and select **Transfer**

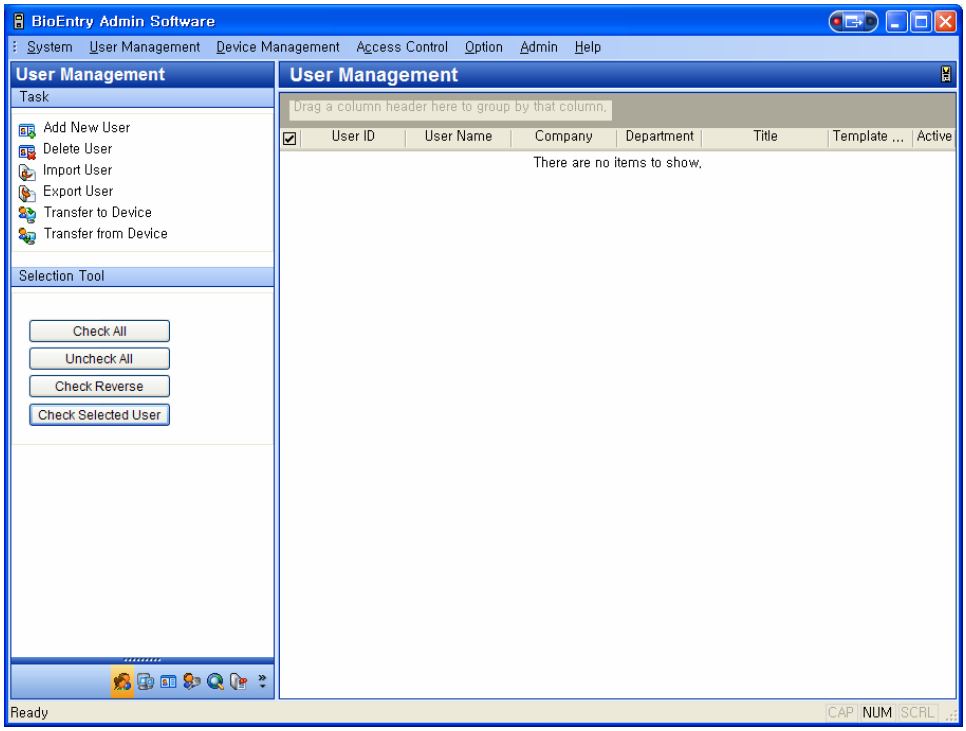
from Device on the task window.

- Select the reader then summarized information is displayed.

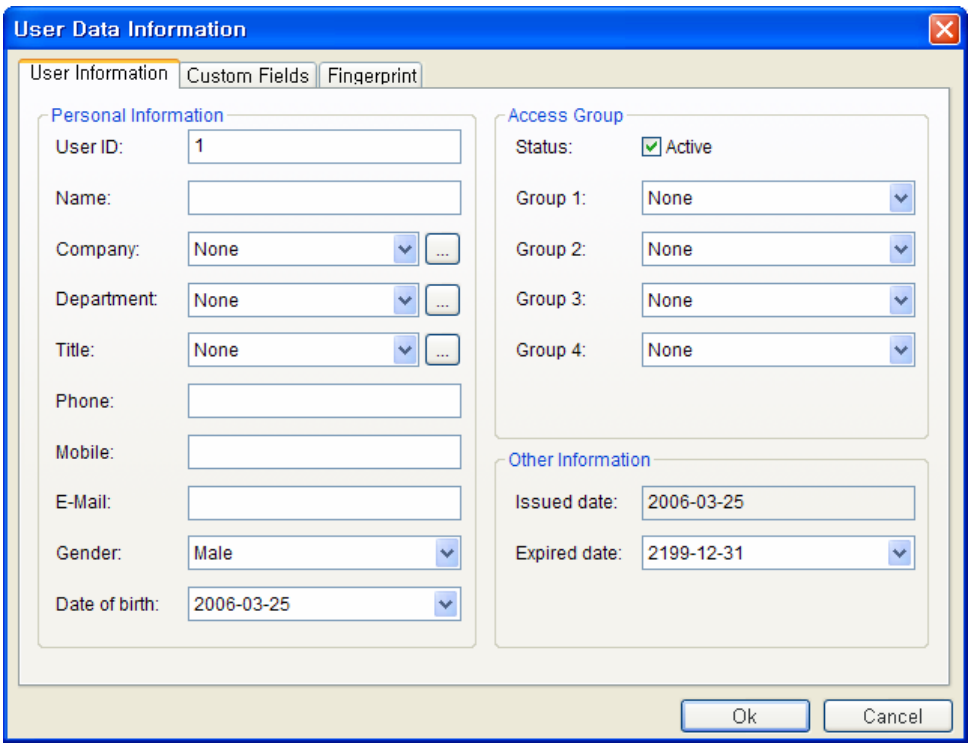


3.3.3. Step 3: Registration of user

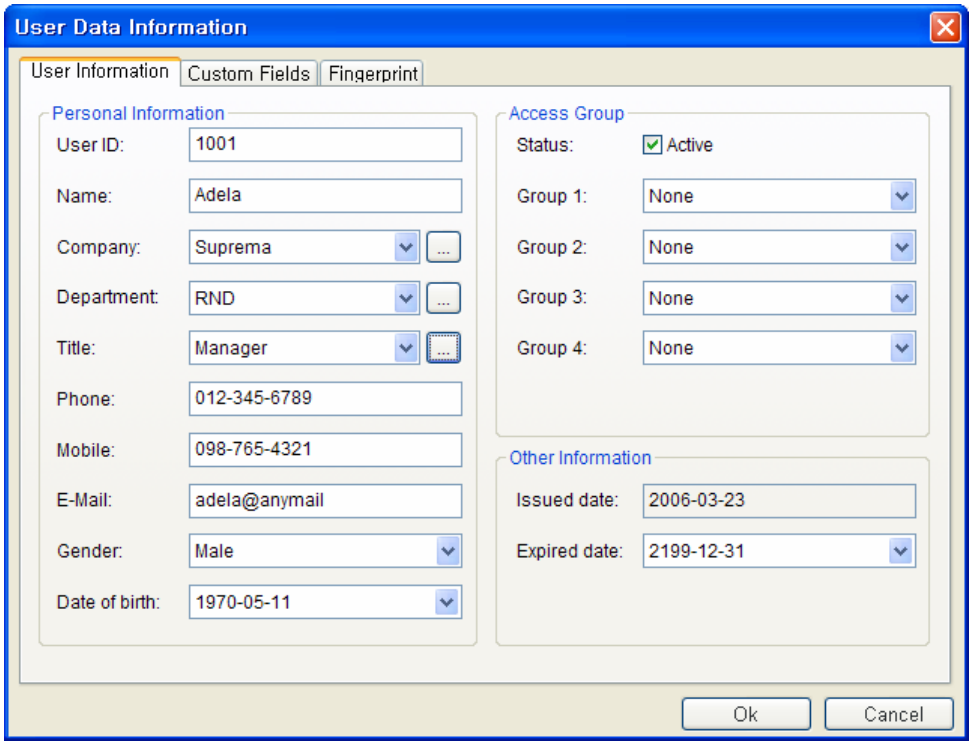
- Select the **User Management** menu, then the user management page appears on the main window



- Select the **Add New User** menu on the task window, then the pop-up window appears.

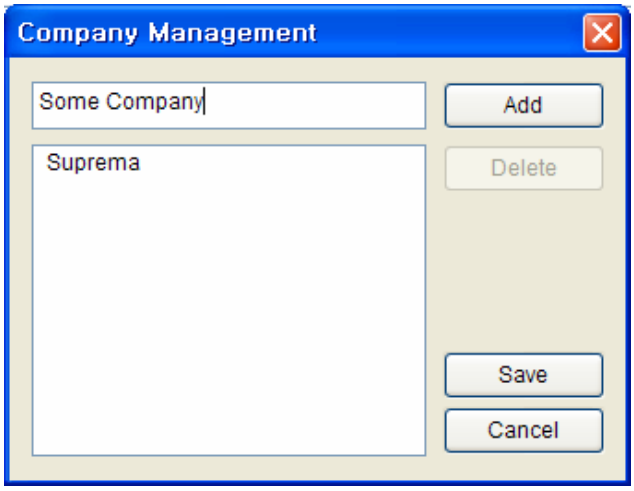


- Enter the user information on the **User Information** tab.



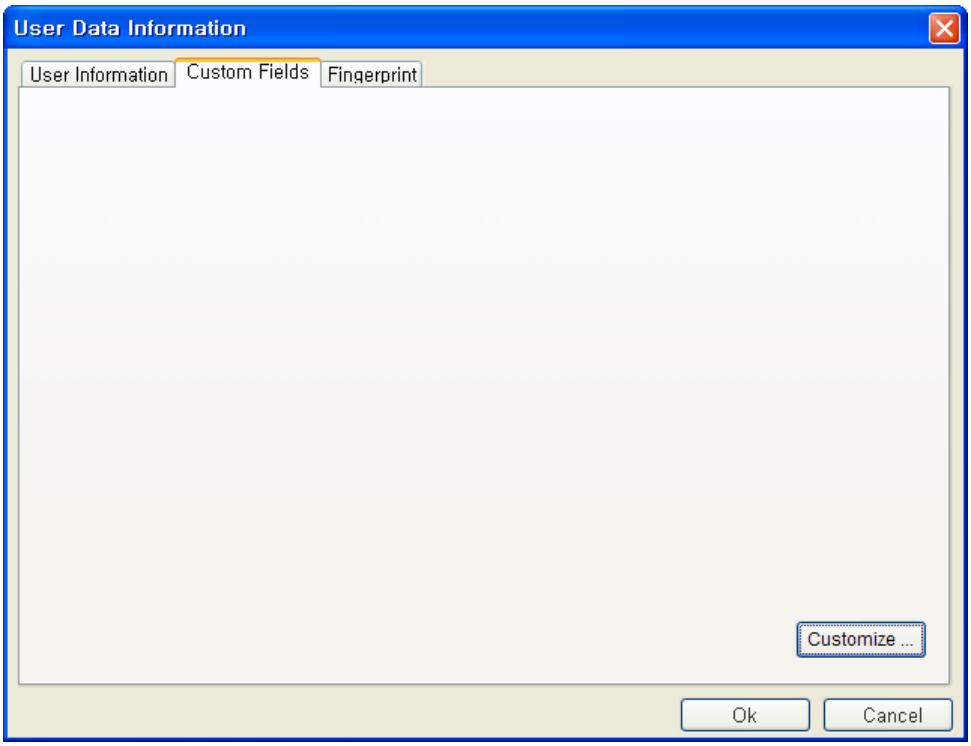
- Especially, you can select the Company, Department, and Title on the drag down menu.
- To add new Company, Department, or Title information, press the button. After entering the required information, press the **Add** button.

  Press the **Save** button to save the added information.



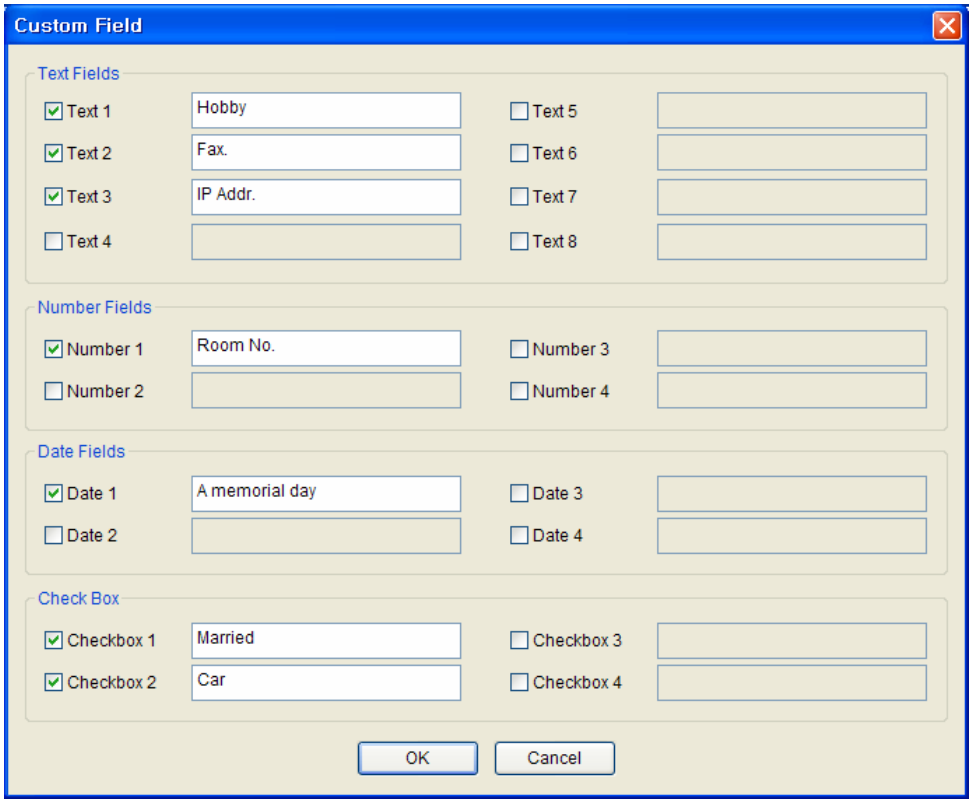
- In addition to the basic user information, you can add the **Custom Fields** to the user information. If you do not need these custom fields, just skip the custom fields setting.

  To set up the custom fields, press the **Custom Fields** tab.

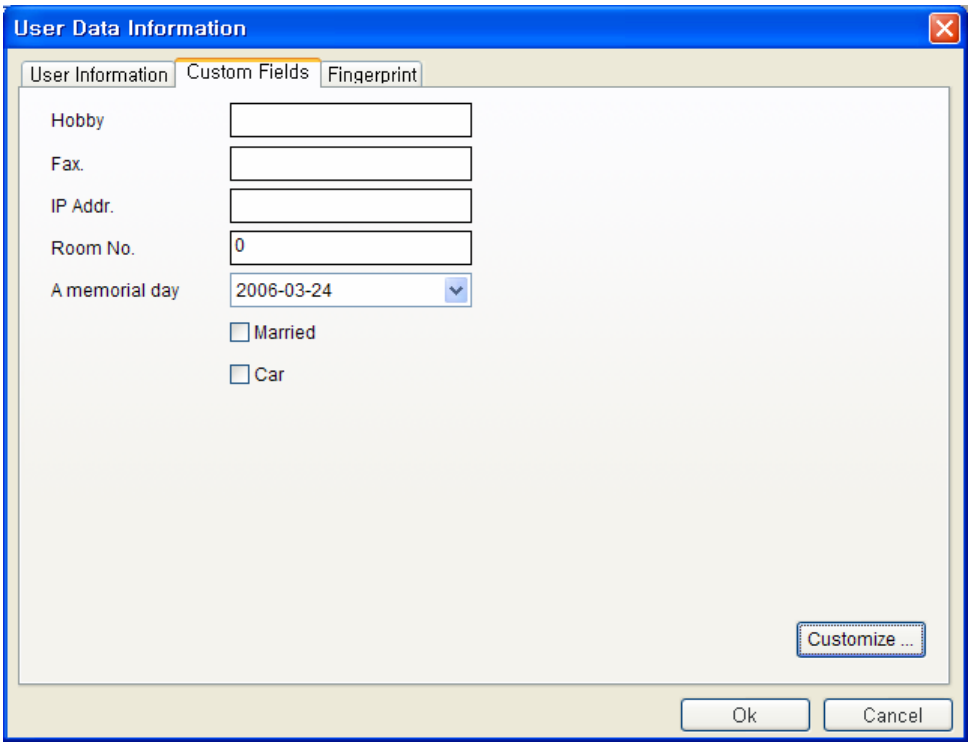


- Click the **Customize...** button.
- Check on the required fields and enter the user information for those selected fields.

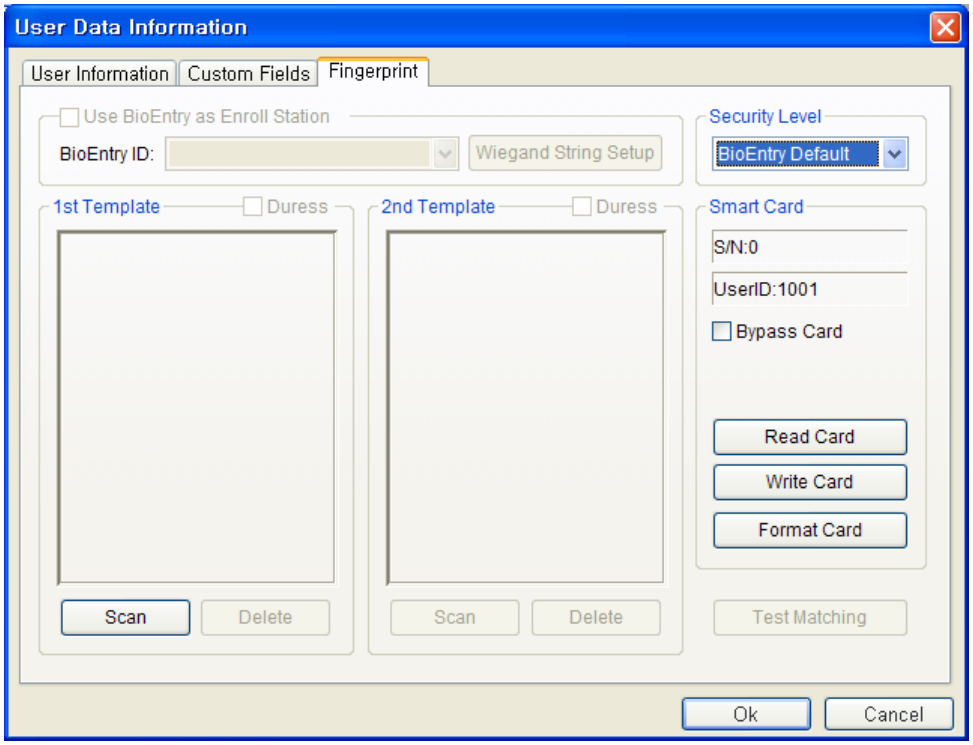
- After entering the user information, press the **OK** button.



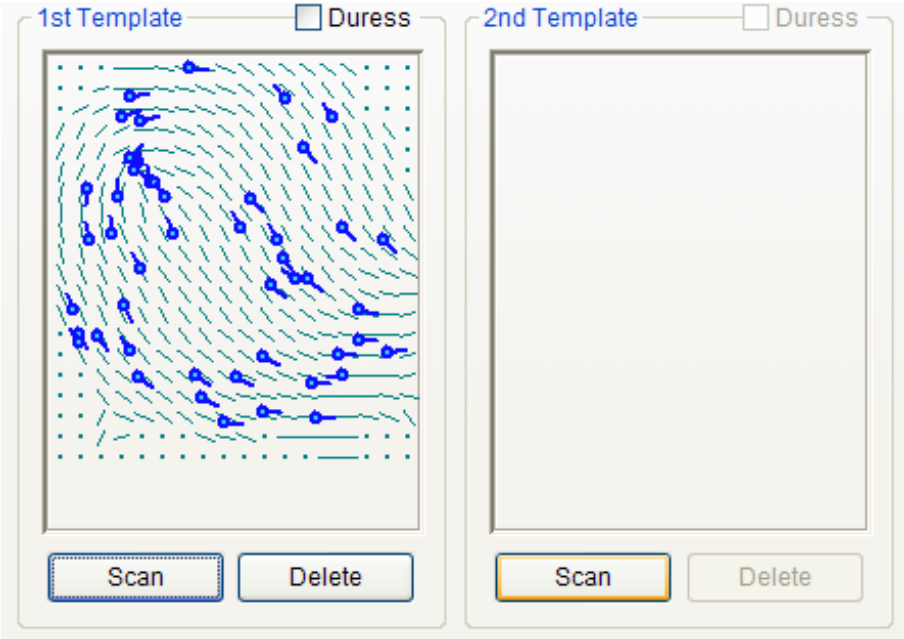
- After filling out the custom fields, following the pop-up window will appear. On this window, you can see the detail of your selected custom fields. Press the **OK** button to save these custom fields.



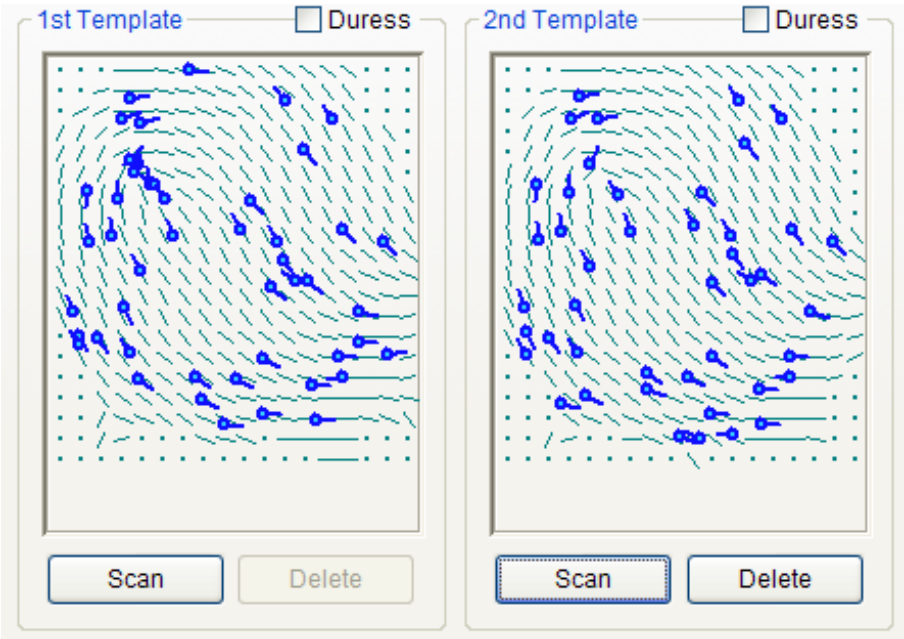
- After entering the user information, press the **Fingerprint** tab to enroll user's fingerprint templates.



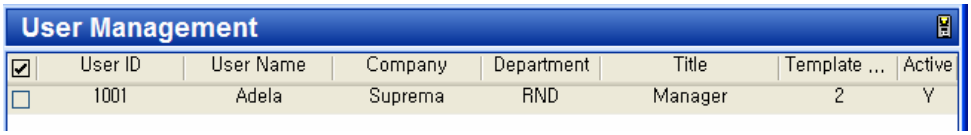
- Acquire first template by pressing the **Scan** button followed by touching a finger on the USB fingerprint scanner twice.



- Acquire second template similarly to the acquisition of first template.



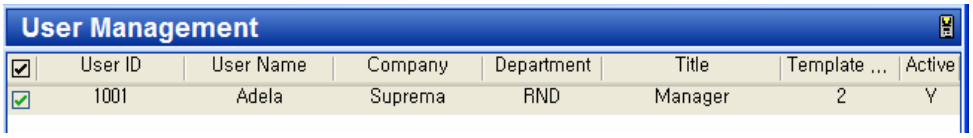
- Press the **OK** button to complete the registration process. Then, you can see the information on the registered user on the user list window. It means that the user's information is added to the database on host PC.



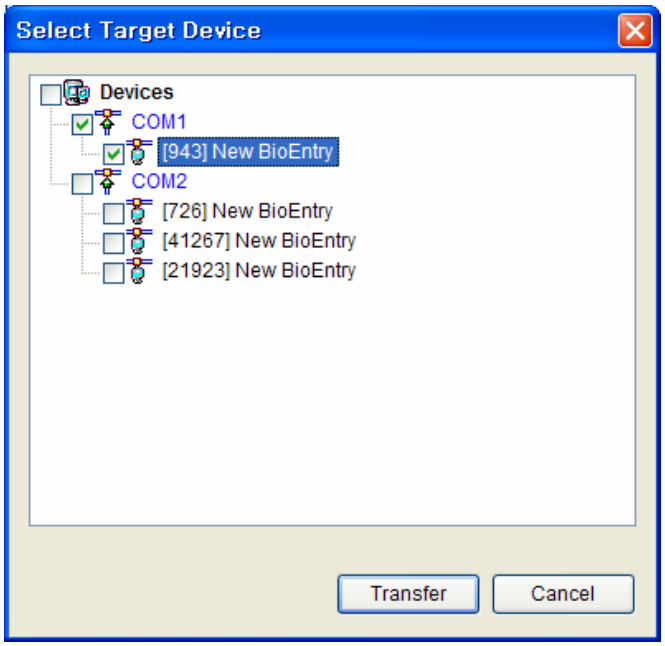
3.3.4. Step 4: Enrollment of user by the Transfer to Device menu.

Transfer to Device is used to transmit the user database of the host PC to BioEntry™ readers. The user information such as User ID, templates, access group, and security level is transferred by this process.

- Check the registered user.



- Press **Transfer to Device** button and check device to transfer. Press **Transfer** button.



Press the **Transfer from Device** button and click the device. If the user information area is highlighted with yellow color, it means that the user information is successfully transferred to the device.

3.3.5. Step 5: Register user ID on the external controller

It is required that the issued user ID is also registered to the external controller to grant access when the Wiegand string for the user is received.

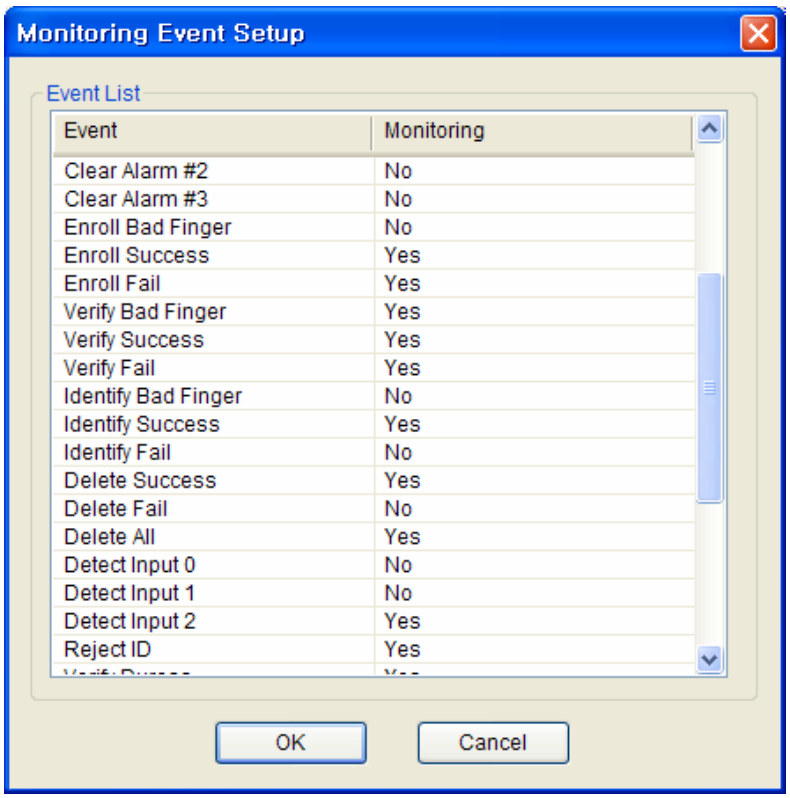
If you are using Suprema's BEACon™ controller, you can just skip this additional registration to the controller.

3.3.6. Step 6: Test identification

- Amber LED on the reader blinks slowly indicating that the reader is waiting for finger scan for identification.
- Swipe finger on the sensor. If the user is successfully identified steady green LED appears with one beep sound. Otherwise, red LED appears with 3 beep sounds.
- On successful identification, the Wiegand string is also sent to the controller, which can be checked by operation of relay on the controller.

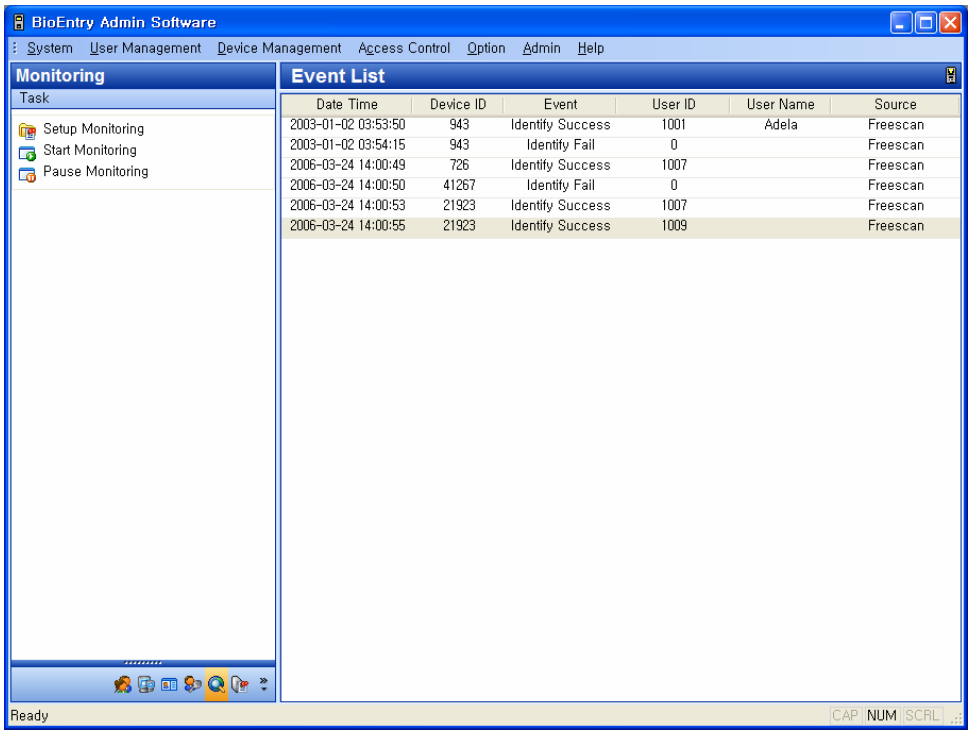
3.3.7. Step 7: Monitoring Event

- Select the **Monitoring** menu. Then, the event list window appears on the main window.
- Select the **Setup Monitoring** menu, and double click to turn on or off the event to watch. Press the **OK** button to save.



Event	Monitoring
Clear Alarm #2	No
Clear Alarm #3	No
Enroll Bad Finger	No
Enroll Success	Yes
Enroll Fail	Yes
Verify Bad Finger	Yes
Verify Success	Yes
Verify Fail	Yes
Identify Bad Finger	No
Identify Success	Yes
Identify Fail	No
Delete Success	Yes
Delete Fail	No
Delete All	Yes
Detect Input 0	No
Detect Input 1	No
Detect Input 2	Yes
Reject ID	Yes

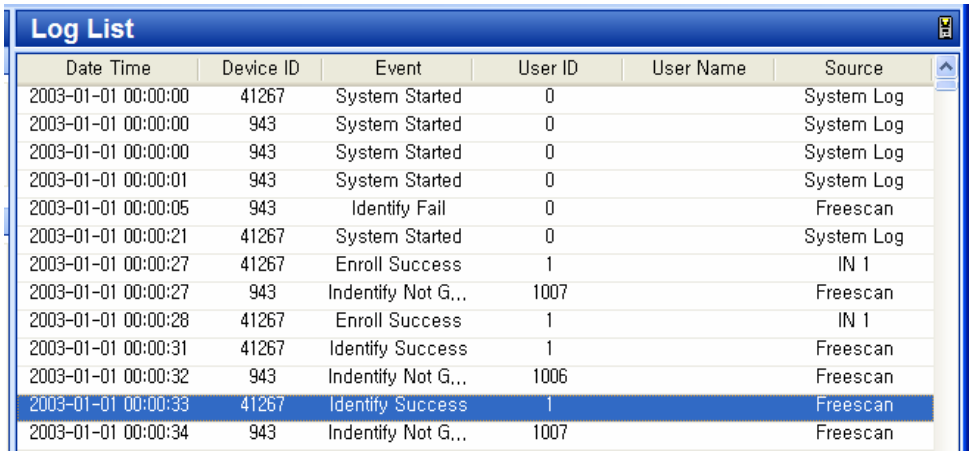
Select **Start Monitoring** menu to start the real-time monitoring on all of the connected BioEntry™ readers.



Date Time	Device ID	Event	User ID	User Name	Source
2003-01-02 03:53:50	943	Identify Success	1001	Adela	Freescan
2003-01-02 03:54:15	943	Identify Fail	0		Freescan
2006-03-24 14:00:49	726	Identify Success	1007		Freescan
2006-03-24 14:00:50	41267	Identify Fail	0		Freescan
2006-03-24 14:00:53	21923	Identify Success	1007		Freescan
2006-03-24 14:00:55	21923	Identify Success	1009		Freescan

3.3.8. Step 8: Check log

- Select the **Reports** menu. Then, the report list window appears on the main window.
- Press the **Upload Log** button. Then, you can see the event log data on the reader which is added to the log database on host PC.



Log List

Date Time	Device ID	Event	User ID	User Name	Source
2003-01-01 00:00:00	41267	System Started	0		System Log
2003-01-01 00:00:00	943	System Started	0		System Log
2003-01-01 00:00:00	943	System Started	0		System Log
2003-01-01 00:00:01	943	System Started	0		System Log
2003-01-01 00:00:05	943	Identify Fail	0		Freescan
2003-01-01 00:00:21	41267	System Started	0		System Log
2003-01-01 00:00:27	41267	Enroll Success	1		IN 1
2003-01-01 00:00:27	943	Indentify Not G...	1007		Freescan
2003-01-01 00:00:28	41267	Enroll Success	1		IN 1
2003-01-01 00:00:31	41267	Identify Success	1		Freescan
2003-01-01 00:00:32	943	Indentify Not G...	1006		Freescan
2003-01-01 00:00:33	41267	Identify Success	1		Freescan
2003-01-01 00:00:34	943	Indentify Not G...	1007		Freescan

3.4. Placing fingers on the sensor

It is important to place fingers properly on the sensor for successful operation of BioEntry™ readers. Authentication performance improves dramatically by proper placement of fingers.

3.4.1. Placing fingers on area type sensors

Please be sure that the finger is placed at the center of sensor and flat to the surface of sensor.

- Proper placement

The following figure shows an example of proper placement on the sensor.

- Improper placement

The following figure shows examples of improper placements.

3.4.2. Scanning fingers on swipe type sensor

In scanning fingers on swipe type sensor, be sure that whole finger is swiped downward by placing the finger flat over the sensor starting from the finger joint.

- Proper placement

- Improper placement

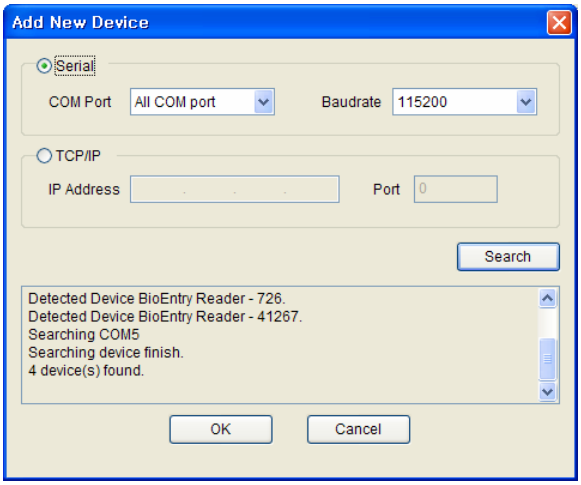
4. Networking BioEntry™ readers

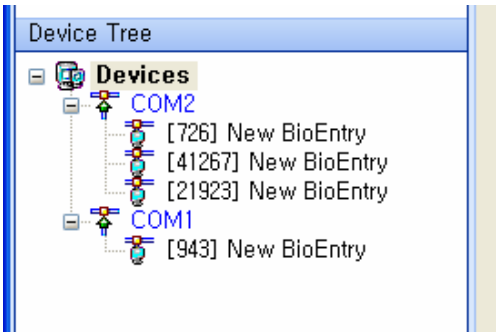
Networking is the initial set up to integrate the BioEntry™ readers into the application system. The network window on BioAdmin software shows current network configuration. For proper hardware connection of the BioEntry™ readers with host PC, refer to *BioEntry™ Installation Guide.*

4.1. Add and remove reader

4.1.1. RS422/485

New reader on the RS422/485 network can be automatically detected and added by the **Search Reader** menu in **Device Management**. If the reader is properly connected to the network, the reader ID will appear with bracket [****] below the port on the device tree window.

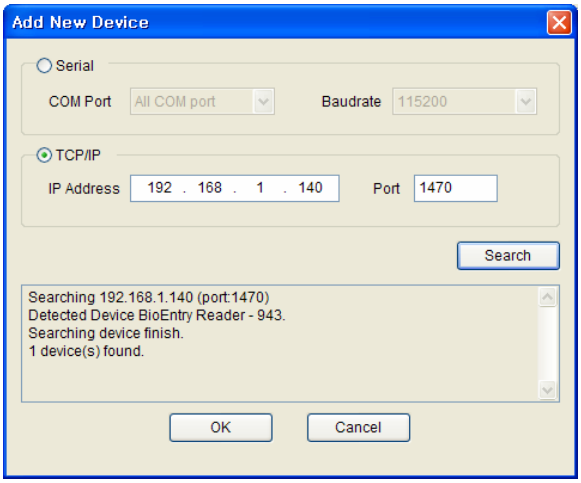




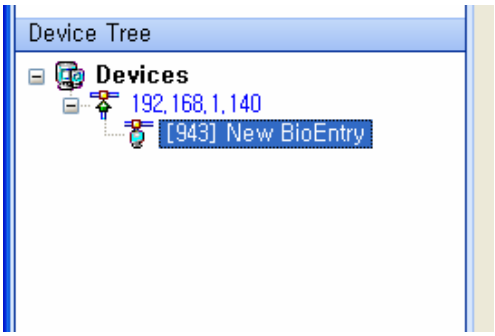
Though the reader is disconnected from the network, it still exists on the device tree window. The **Remove Devices** menu or **Remove Reader** menu eliminates the reader from the network window.

The name of the reader can be specified by the **Rename Reader** menu. Reader ID is fixed and cannot be changed.

4.1.2. Ethernet



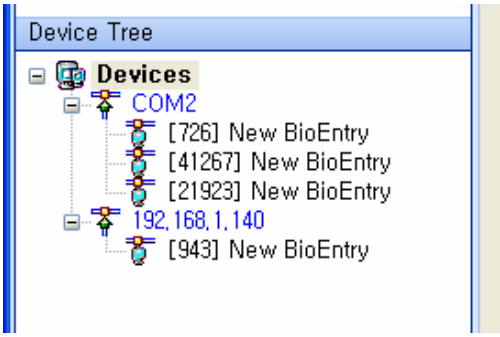
Users can connect BioEntry™ readers using serial-to-Ethernet converters. To use a serial-to-Ethernet converter, users should know its IP address and port number. If the reader is properly connected, its IP address will appear as a group and the reader ID will appear with bracket [****] on the device tree window.



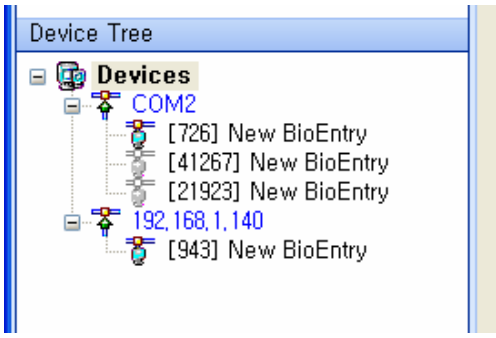
4.2. Reader status

Current status of the reader is discriminated by the shape of reader icon on the device tree window.

- If the reader is connected, the icon is highlighted.



- If the reader is disconnected, the icon remains grayed.



The status of each reader is updated in the following cases:

- When the software is started, the status of all readers is updated.
- When a reader is newly selected, the data is retrieved from the reader, or the command is sent to the reader.
- When the **Check Status** menu is initiated.

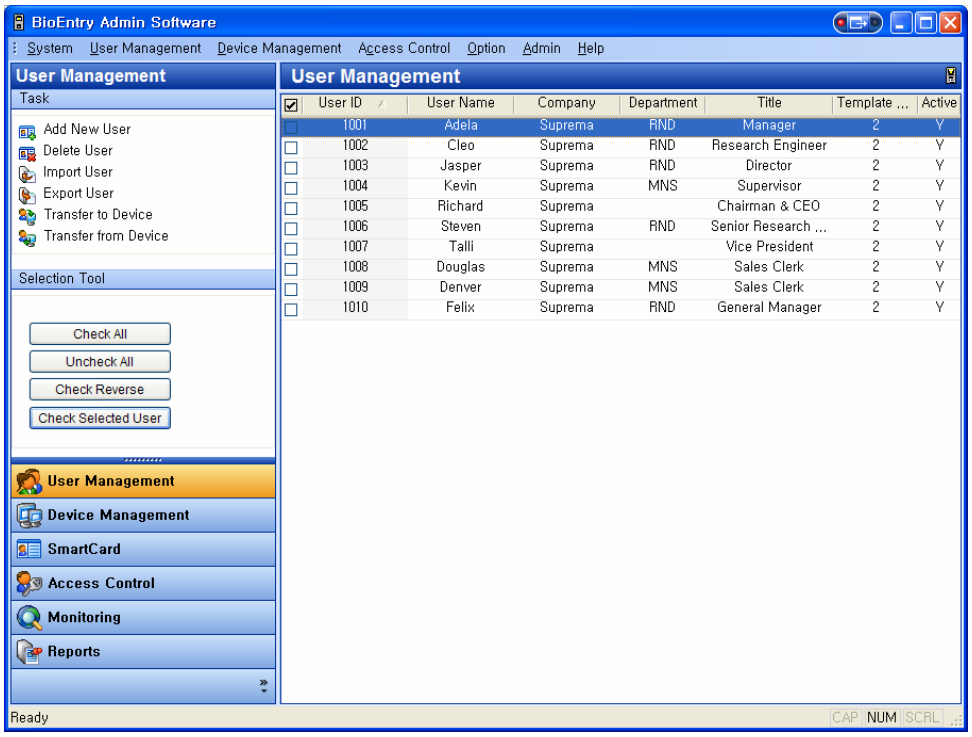
5. User Management

User management covers the following operations:

- Add new user
- Delete user
- Import user
- Export user
- Transfer to device
- Transfer from device
- Management of user's smart card.

5.1. Organization of user management page

By selecting **User Management** menu, user management page is updated on the main window.



The user management page is divided into 3 sectors:

- User List

The user database is under central management on host PC. The user management page includes detailed list of user database and summarized information.

- Selection tool box

Selection tool box includes buttons to select users.

- Task box

Task box includes buttons to control basic operations of the user management page.

5.2. User List

User list includes the following information on the users.

- User ID
- Subsidiary information including name, company, department, title, gender, e-mail address, mobile phone number, access group, date of birth, issuing date, expiry date, number of enrolled templates, and card number.
- Serial number of smart card
- Customized user information
- Fingerprint templates (fingerprint image is never stored)

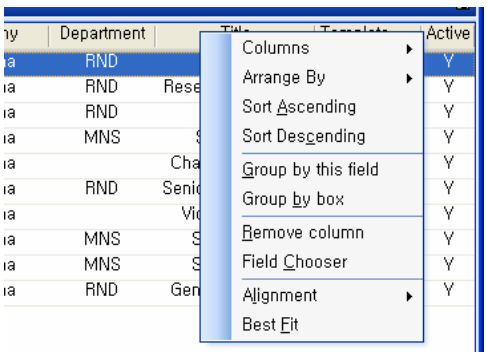
When a reader is selected, user list is updated to indicate the consistency of the user data between reader and host database.

5.3. User List Display Set up

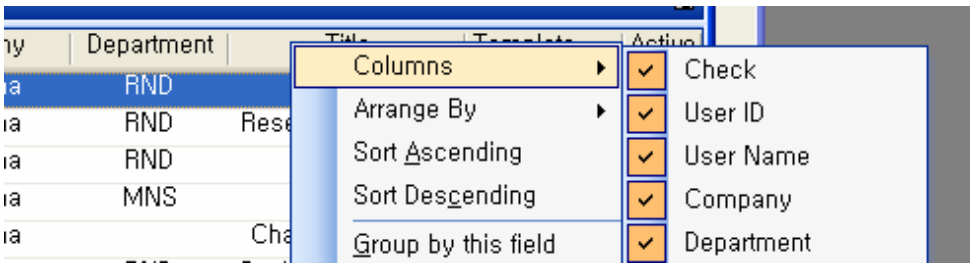
You can customize the display of the user list.

Detailed operations are as follows.

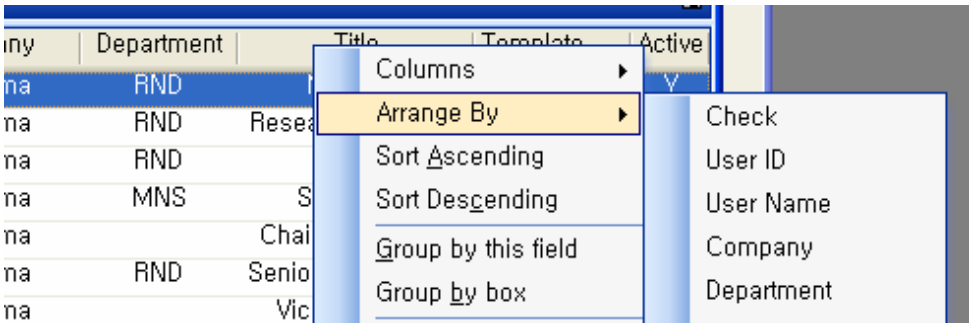
- Press the right button of your mouse on the column header of User List.



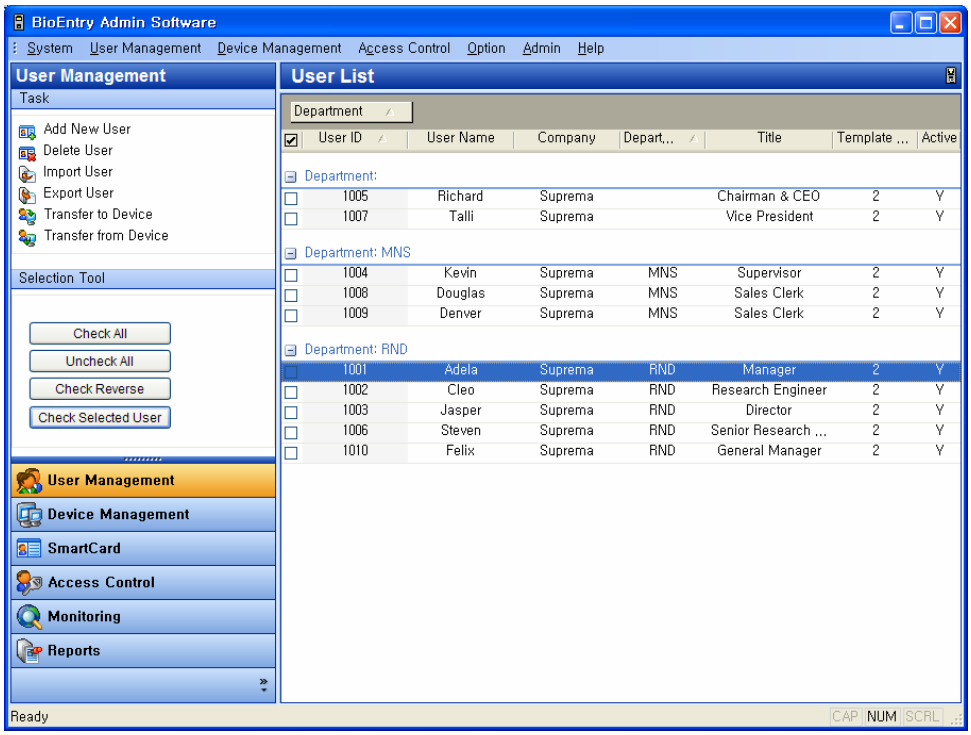
- Press the **Columns** button and check on your required columns to show them on the user list.



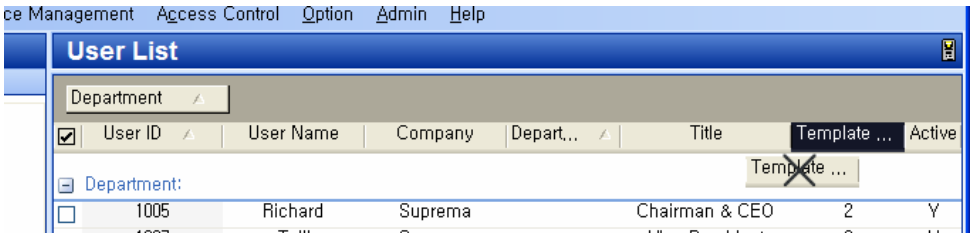
- Press the **Arrange By** button and select your required columns to array the user list by your selected column.



- Press the **Sort Ascending** button to array the user list in ascending order.
- Press the **Sort Descending** button to array the user list in descending order.
- Press the **Group by this field** button and **Group by box** button to manage the user list as a group by your required columns. Also, you can add a column to the group simply by dragging up the column to the header box.



- Press the **Remove Column** button to remove a column from the header. Also, you can remove a column simply by dragging down the column from the column header.

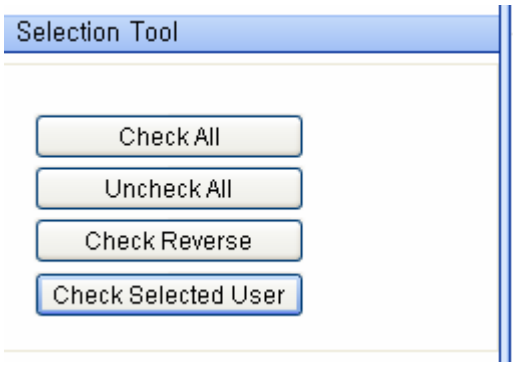


- Press the **Alignment** button to array the content in your preferred way.
- Press the **Best Fit** button to optimize the width of a column.

5.4. Selection of users

Users can be chosen for selective processing of operations, such as transfer, removal, or exportation. You can select the required user simply by using the check box on the user list,

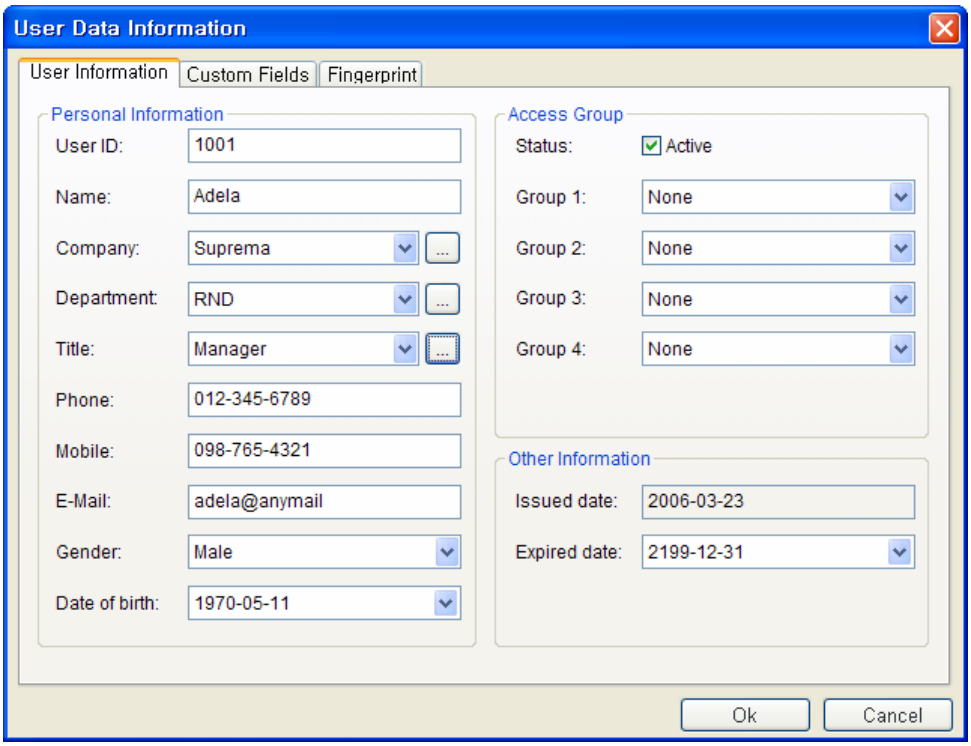
Also, selection tools can be used for easy user selection.



- Check All : Check all users
- Uncheck All : Uncheck all users
- Check Reverse : Check all users except the users who were originally checked
- Check Selected User : Check the selected user

5.5. Add New User

The **Add New User** button enables the pop-up window to register user data on host PC.

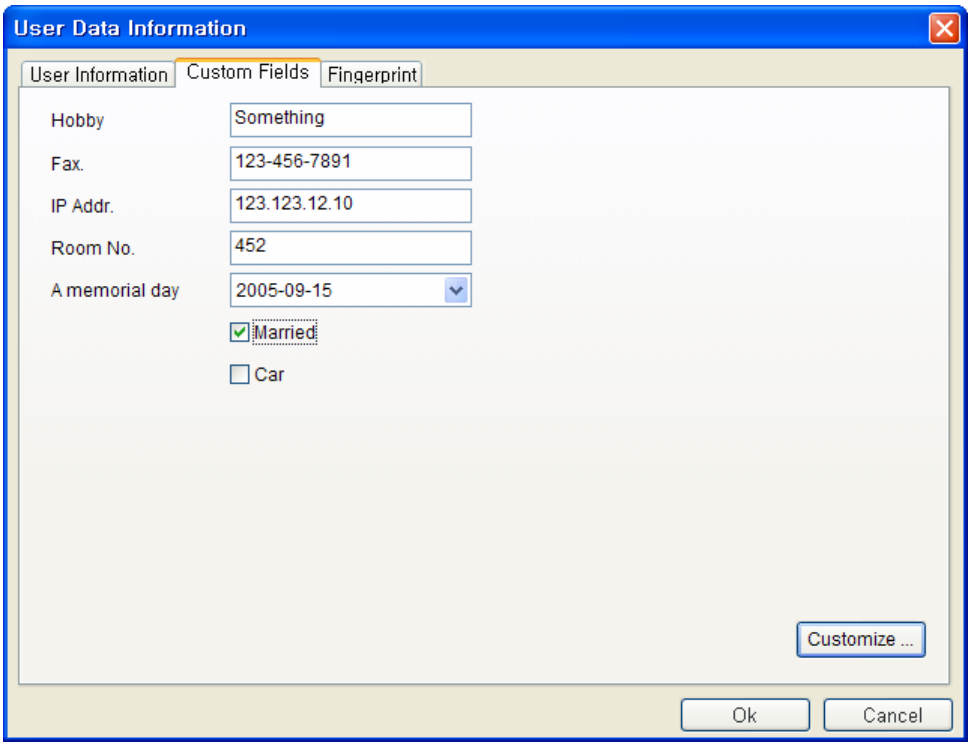


- User Information

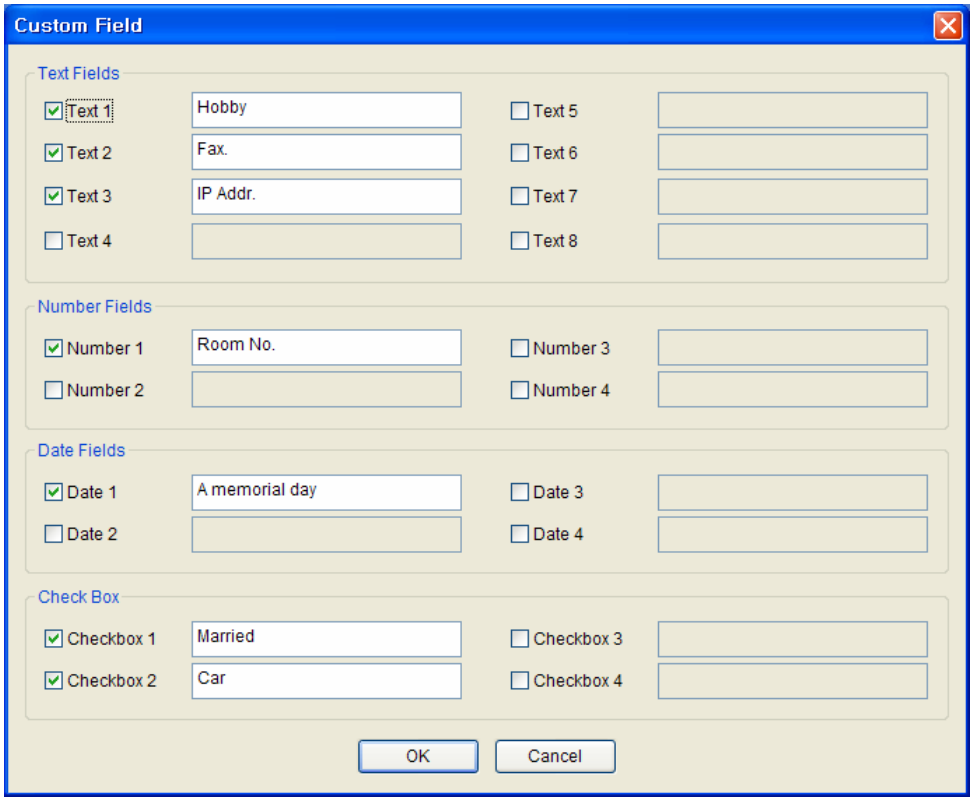
After filling out user information, press the **OK** button.

- Custom Fields

You can add customized user information columns on the user management window by designating required fields on the **Custom Fields** menu.

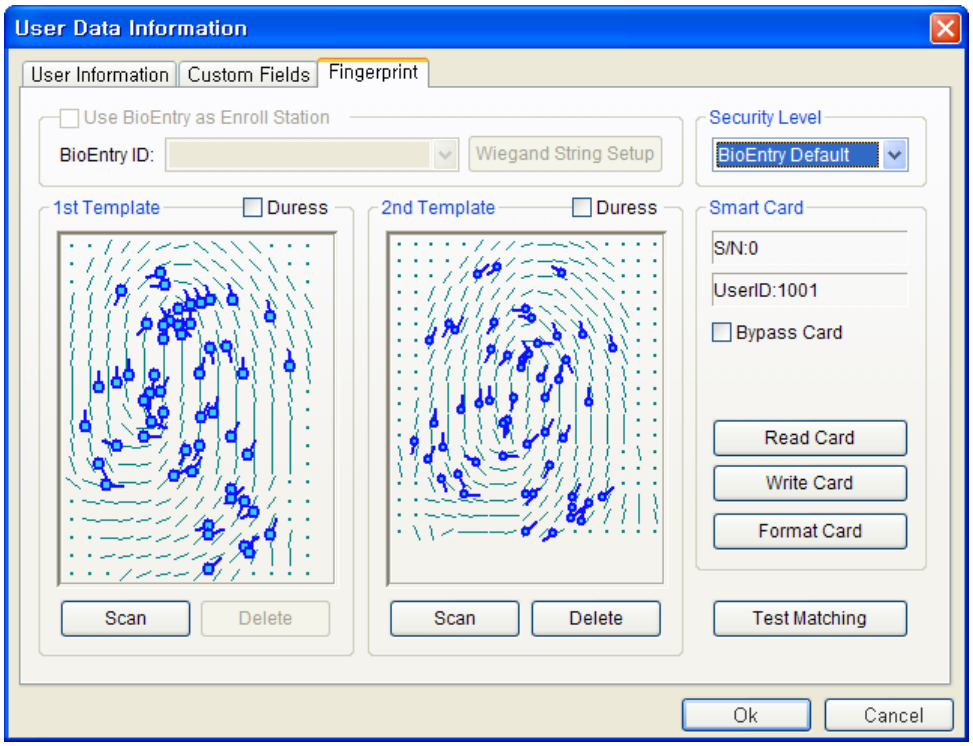


Customize… button enables the pop-up window to add the customized user information column. After filling out the required contents, press the **OK** button.



5.5.1. Enrollment

The next step of registration is adding user's fingerprint templates to database.



Templates can be enrolled by two methods:

- Enrollment using PC USB scanner
- Enrollment using BioEntry™ reader connected to host PC

By default, USB scanner is used for enrollment. By enabling the **Use BioEntry as Enroll Station** check box and selecting a reader ID, BioEntry™ reader is used to get user's templates. Up to 2 fingerprint templates can be included in the user database.

- Acquisition of template

Press the **Scan** button and touch the same finger twice. If the acquisition of template is successful, scanned template is depicted on the template window. To register the second template for different finger, press the **Scan** button at the right section.

- Enrollment of duress finger

Duress finger can be enrolled to generate duress signal when the specified finger is detected on the reader. After a template is acquired, enable the **Duress** check box to indicate that the template should be saved as duress mode.

- Test matching

In order to check that enrollment of template is properly completed, matching test can be processed. Press the **Test Matching** button and touch the registered finger on the specified reader. Then, a message will appear to show the matching result.

5.5.2. Issuing user's smart card

BioEntry™ Smart basically operates with user's smart card containing user information and fingerprint templates. Issuing is required to create the user's smart card.

Issuing of user's smart card is processed on the user management window, which is initiated by double clicking a user on the user list or by pressing the **Register New User** button on the main window.

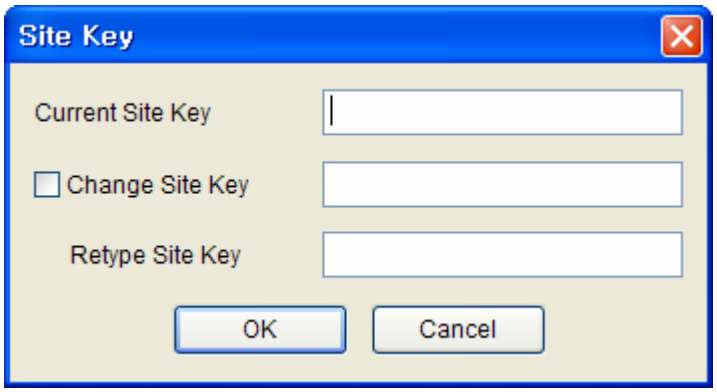
Smart card can be issues by two methods:

- Issuing with PC USB smart card reader
- Issuing with BioEntry™ Smart connected with host PC

To use a BioEntry™ Smart as a card issuer, enable the **Use BioEntry as Enroll Station** check box and select a reader ID. Otherwise, PC USB reader is used as a card issuer.

5.5.3. Issuing with PC USB smart card reader

- Place the target smart card on the PC smart card reader
- Press the **Write** button to initiate issuing.
- The site key management window will appear at the first trial of issuing after starting of BioAdmin software. Also, the window will appear if it fails to access the smart card due to the mismatch of the site key.



- Type the current site key to access the smart card. If it remains blank, BioAdmin software uses default key (0xFFFFFFFFFFFF) as a current site key.
- If it is desired to change the site key on issuing, enable the **Change Site Key** check box and type new site key. Then, new site key is updated on the smart card. The new site key should be correspondent with the site key on BioEntry™ Smart reader. Please refer to Chapter 11. Site Key for managing site key for BioEntry™ reader.

5.5.4. Issuing with BioEntry™ Smart

- Place the target smart card at selected BioEntry™ Smart
- Press the **Write** button to initiate issuing. Since the site key management information is stored on BioEntry™, issuing is processed without requesting site key. Please refer to Chapter 11. Site Key for managing site key for BioEntry™ reader.

5.5.5. Specifying user's security level and Bypass

On issuing, security level can be specified for each user. By changing Security Level dropdown list, user's security level can be specified from 1/1,000 to 1/100,000,000. If **BioEntry Default** is selected, security level configured on BioEntry™ Smart reader is used.

The **Bypass** option is included in Security Level to issue a bypass card. With a bypass card, user is always granted for access just by placing the bypass card to BioEntry™ reader, without touching finger,

5.5.6. Specifying Wiegand string using ID card

On issuing a smart card, the specific Wiegand string contained in customer's ID card can be transferred to the smart card. For this operation, RF Wiegand reader should be connected to the Wiegand input port of the selected BioEntry™ reader.

Detailed operations are as follows.

- Press the **Wiegand String Setup** button
- Press the **Get Wiegand String** button and touch the ID card containing

Wiegand string on the Wiegand reader.

- The Wiegand string received from the reader is displayed on the user management window.
- Enable **Write Wiegand String As It is** check box to use the Wiegand string instead of the user ID
- Press **OK** button to issue the user's smart card. Then, the received Wiegand string is stored on the smart card. If the check box is disabled, the Wiegand string converted from user ID is written to the smart card.

5.5.7. Reading issued smart card

The information stored on the issued smart card can be retrieved by **Read Card** button on the user data information window. When PC USB smart card reader is used, the site key management window will also appear if the site key is mismatched. In reading process, the site key change option is neglected.

5.5.8. Formatting smart card

Formatting is the process of erasing issued information on the smart card. The **Format Card** button on the user data information window initiates formatting process. The site key change option is effective in this process.

5.5.9. Important notice in issuing smart card

- **Before writing on a new smartcard, you should format the new smart card first.**
- **Site key is not stored in BioAdmin software to improve the security of the system. It is the necessary for the administrator to remember and keep in secret the custom site key for proper management of the system. Also, please pay keen attention to changing the site key on the smart card.**
- **If writing to smart card is stopped accidentally in issuing process, the smart card might be corrupted and irrecoverable. Be careful to avoid accidental stop in writing smart card.**

5.6. Editing registered user data

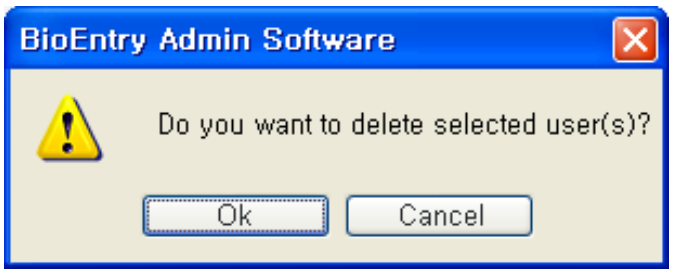
The information of a registered user can be edited simply by double clicking on the user list. User ID, subsidiary user information, and templates can be changed similarly to the registration process.

5.7. Delete User

Registered user can be eliminated by **Delete User** button on user list window.

Detailed operations are as follows.

- Check on the users to delete.
- Press the **Delete User** button.
- The pop-up window appears to confirm whether you really want to delete the selected users.



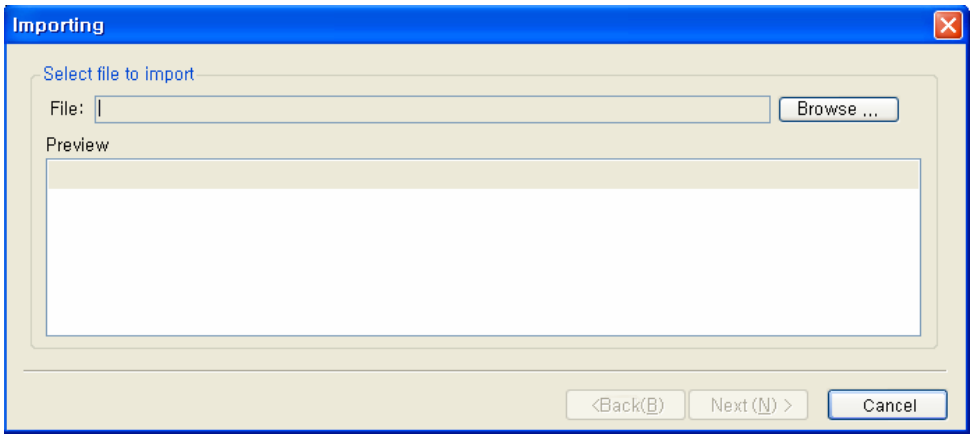
- Press the **Ok** button, if you really want to delete the selected users.

5.8. Import User

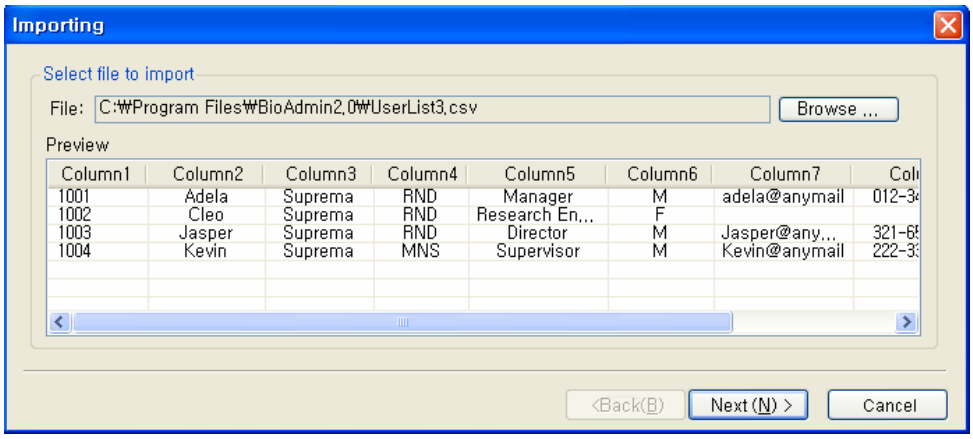
The **Import User** button is used to import user database from an external database to BioEntry™ Admin Software user database. User list saved as CSV (Comma Separated Values) format can be loaded into user database list.

Detailed operations are as follows.

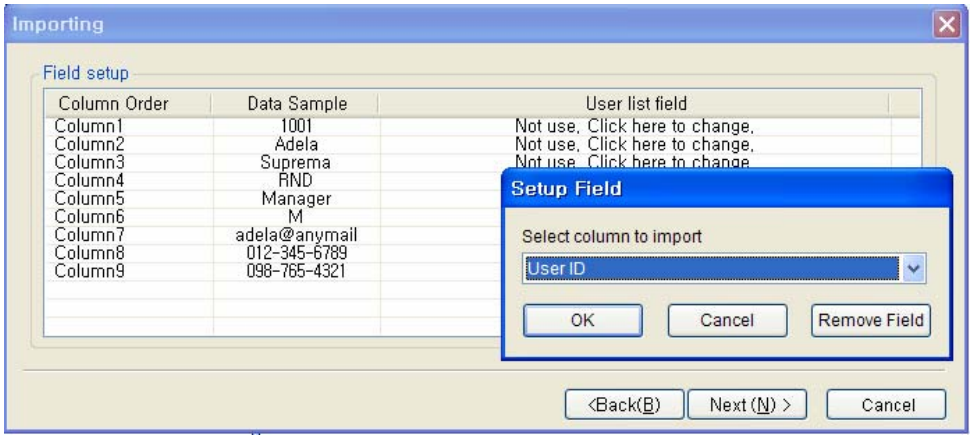
- Press the **Import User** button.



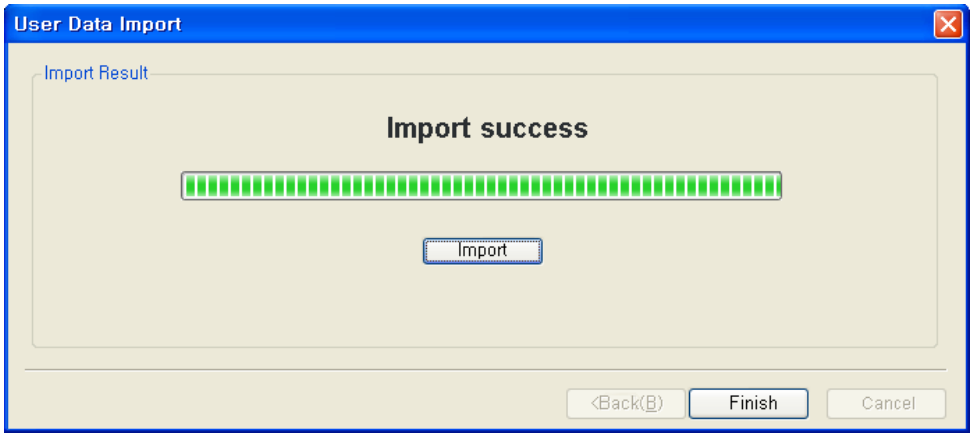
- Select a file to import.
- After selecting the file, you can see the content examples of 5 users on the preview window. Check the preview window to confirm the selected file is the right file from which you want to import the database.



- If the file is correct, press the **Next** button.
- Select a column to import.



- Press the **Import** button.

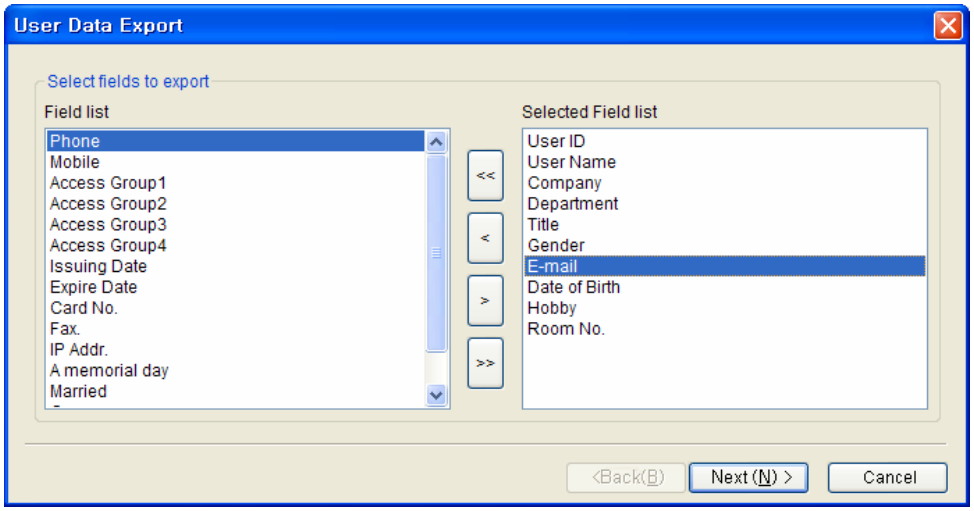


5.9. Export User

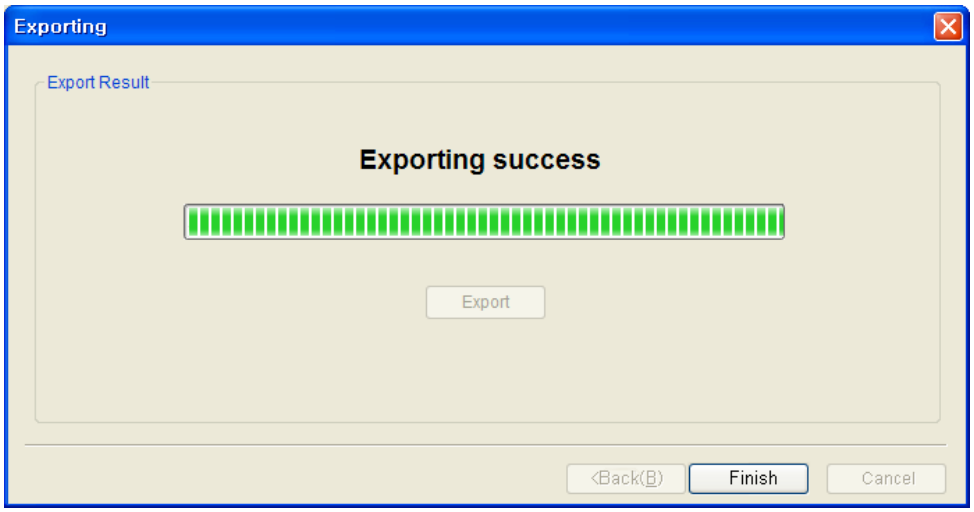
The **Export User** button initiates saving information of selected users in CSV format. Fingerprint templates are not included in this exportation. Exported CSV file can be edited using Microsoft Office Excel or usual text editor.

Detailed operations are as follows.

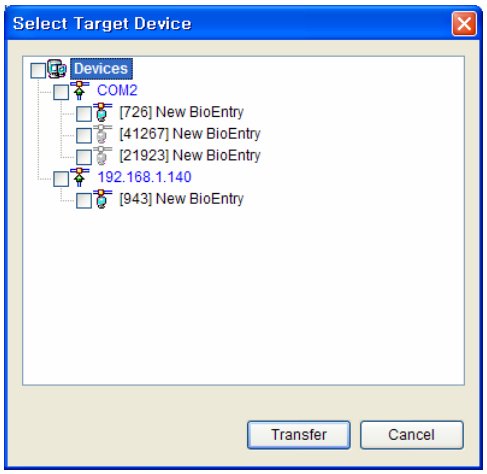
- Check on the users to export.
- Press the **Export User** button.



- Select fields to export. You can select the target fields simply by moving the target fields from Field list to Selected Field list.
- After selecting the fields, press the **Next** button.
- Select a file to export.
- After selecting the file, press **Next** button.
- Press **Export** button.



5.10. Transfer to Device

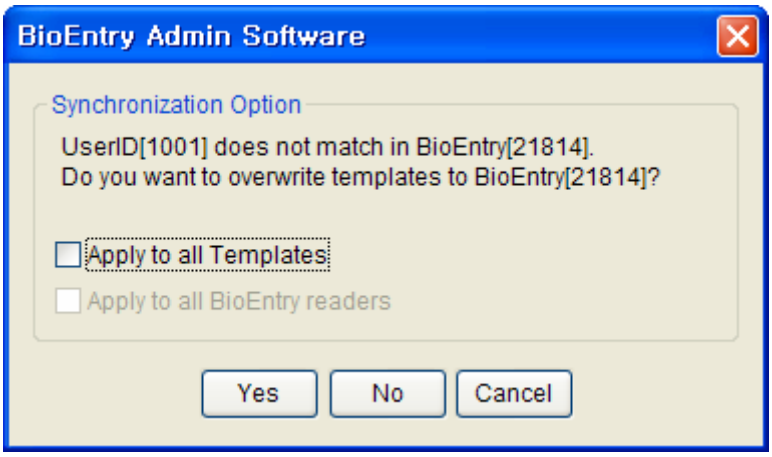


Transfer to Device is used to transmit the user database of the host PC to BioEntry™ readers. In order to operate BioEntry™ Pass, the user data including fingerprint templates should be transferred to the reader after registration of users.

The user information such as User ID, templates, access group, and security level is transferred by this process. Transfer can be processed on a selected reader, a selected group, or all connected readers on the network. Selective transfer of user data is also allowed by user selection method.

Detailed operations are as follows.

- Check on the users to transfer.
- Press the **Transfer to Device** button.
- If selected user is not found on the reader, new user data is transferred to the reader from the host database.
- If user information on BioEntry is inconsistent with that of the host database, following the pop-up window appears.



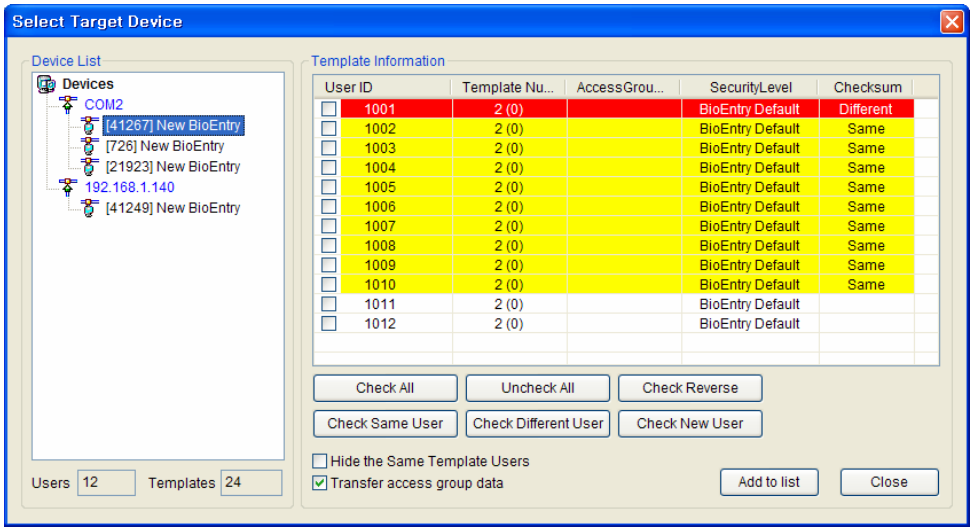
By pressing the **Yes** button, you can replace the user information of BioEntry™ with the new user information from the PC database. By pressing the **No** button, you can keep the original user information of the BioEntry™.

- If the reader contains a user who is not registered or selected on the host database, the user can be eliminated from the reader or kept left.
- On BioEntry™ reader, the minimal information of the user is stored including user ID and templates.

5.11. Transfer from Device

Transfer from Device is used to upload the user formation from BioEntry to the database of the host PC. The user information such as User ID, Template Number, Number of Access Group, and Security Level can be uploaded by this process.

Transfer can be processed from a selected reader on the network. Selective transfer of user data is also allowed by user selection method.

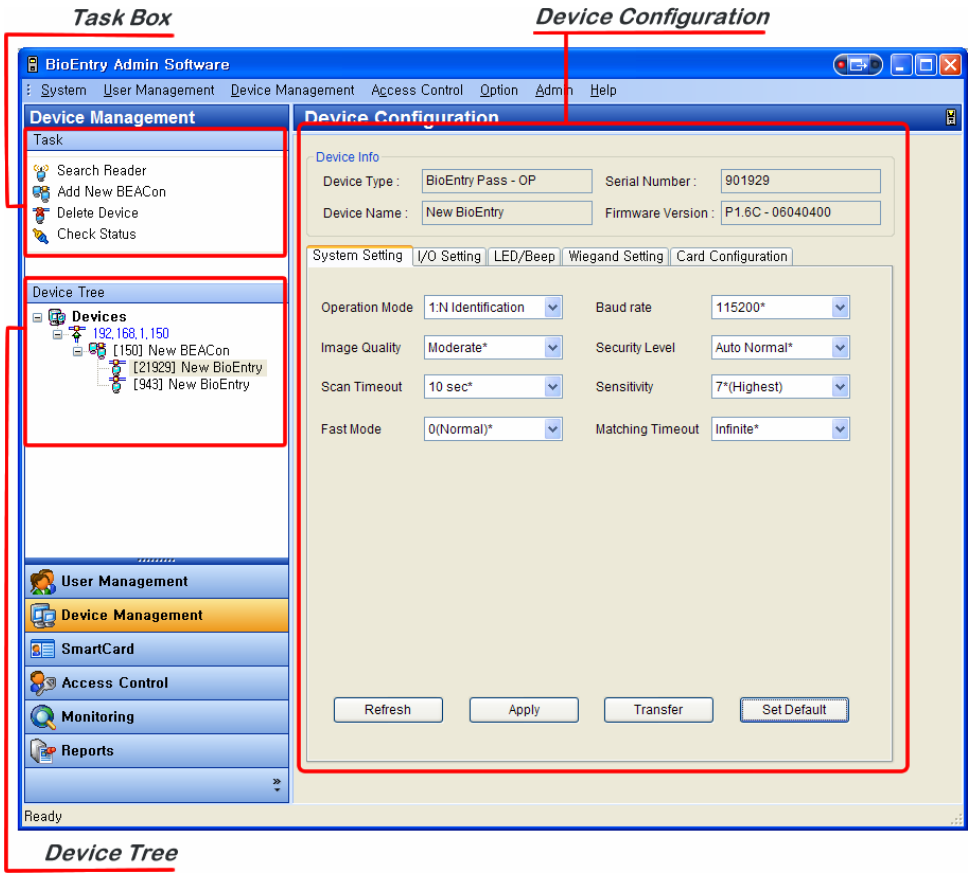


Detailed operations are as follows.

- Press the **Transfer from Device** button
- Click the target BioEntry™ on the Device List window.
- Below the Device List window, you can see the number of users and templates enrolled on the selected BioEntry™.
- For the users whose templates are enrolled only on BioEntry™, not on the database of host PC, user fields on the template Information window will remain without any color.
- For the users whose templates on BioEntry™ are consistent with those of the host database, user fields are highlighted with yellow and **Same** will be shown on the checksum field. By checking on **Hide the same template users,** you can hide these users from the template Information window.
- For the users whose templates on BioEntry™ are not consistent with those of the host database, user fields are highlighted with red and **Different** will be shown on the checksum field.
- By checking on **Transfer access group data**, you can upload user's access group information as well.
- Select target users for transfer.
- After selecting target users on the Template Information window, press the **Add to List** button to upload the information of those selected users.

6. Device Management

By selecting the **Device Management** menu, the device management page is updated on the main window.



Device management page is divided into 3 sectors:

- Device configuration

The configuration set up window shows the current configurations of networked BioEntry™ readers and BEACon™ controllers. Also, this window shows the configurations to be changed.

- Task box

The Task box includes buttons to control basic operations of the Device Management page.

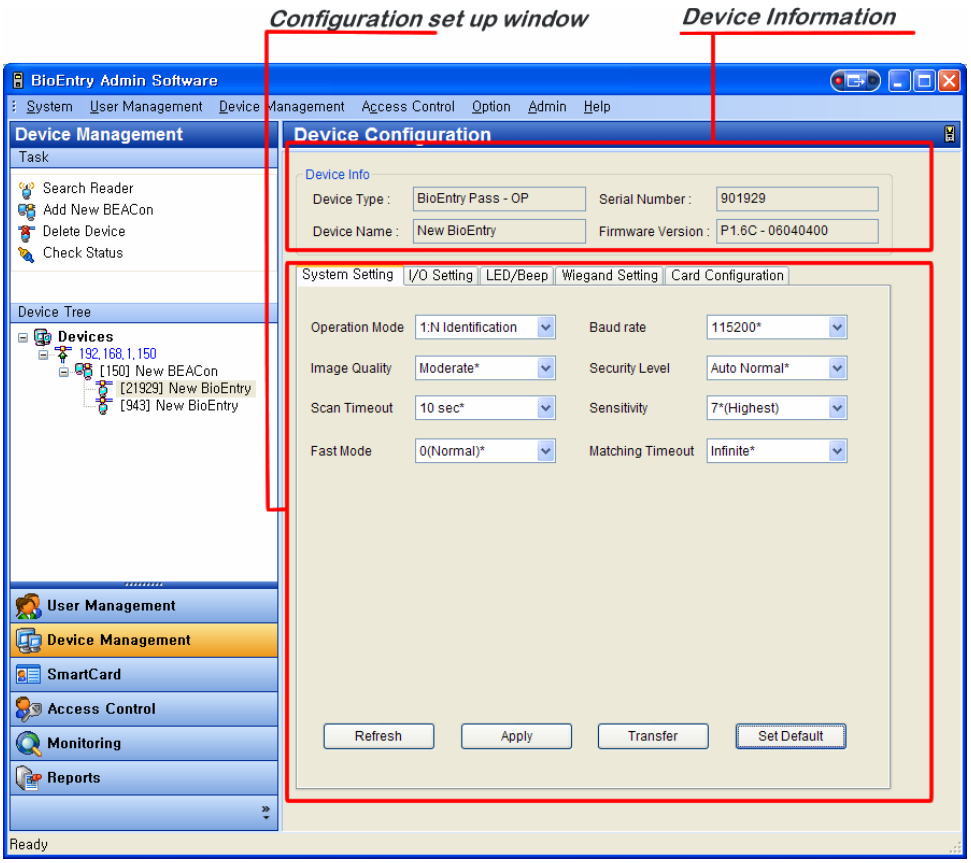
- Device Tree

The Device Tree window shows the network condition of connected BioEntry™

readers and BEACon™ controllers.

6.1. Organization of Device Configuration window for BioEntry™

By selecting a BioEntry™ on the Device tree, the Device Configuration window for the selected BioEntry™ is updated on the main window.



Device Configuration window is divided into 2 sectors:

- Device information

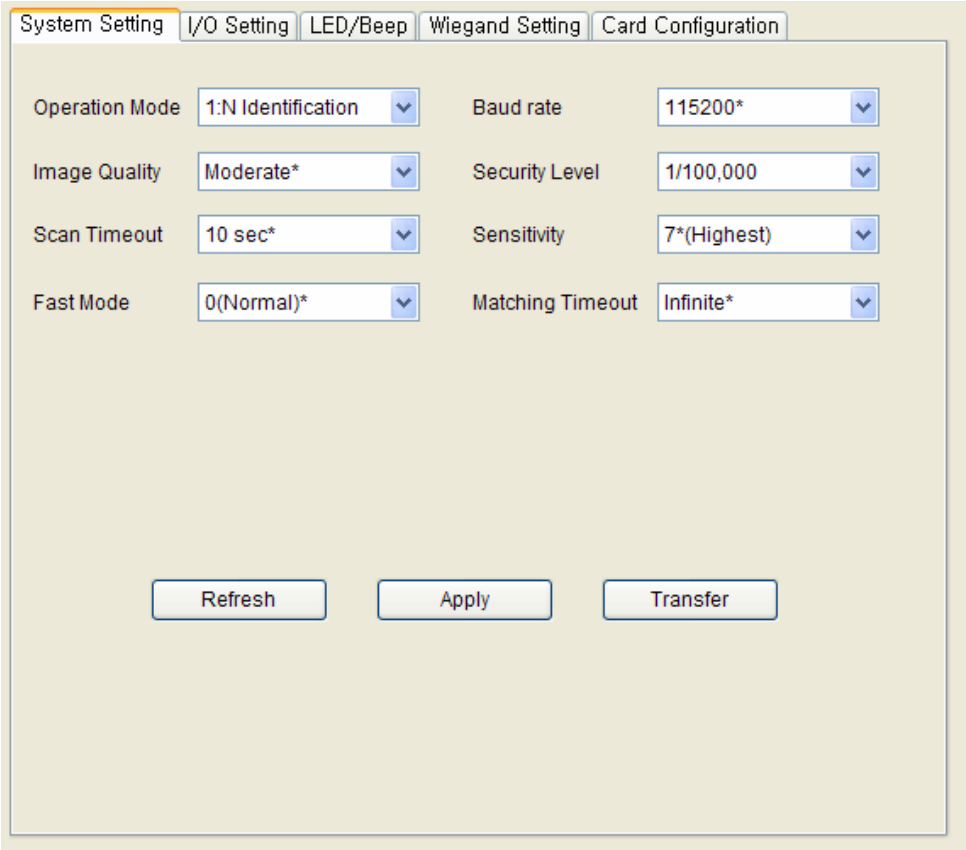
Device information shows the model name, serial number, device name, and firmware version of the selected BioEntry™.

- Configuration Set up window

The configuration set up window shows the current configurations of selected BioEntry™. Also, this window shows the configurations to be changed. The configuration set up menus are divided by separate tabs, such as System setting, I/O setting, LED/BEEP setting, Wiegand setting, Card Layout.

6.2. System Setting

You can set up the parameters of BioEntry™ on the **System Setting** tab. When this tab is selected, the system setting page is updated on the main window.



6.2.1. Operation Mode

- 1:1 Verification

Only verification is supported by BioEntry™ reader. BioEntry™ Smart enters into verification by user's smart card. BioEntry™ Pass enters into verification by the Wiegand input from external reader such as magnetic card reader or ID card reader.

- 1:N Identification

Only identification is supported by BioEntry™ reader. Both BioEntry™ Smart and BioEntry™ Pass continuously wait for finger touch and process identification when a finger is detected.

- Both

Both 1:1 verification and 1:N identification are supported.

6.2.2. Baud rate

Baud rate is the number of times per second that the carrier signal value changes state. If you have some problems to communicate with BioEntry™ reader, changing baud rate to lower value can be a solution.

6.2.3. 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 Ratio) is in inverse proportion to each other, FRR will increase with higher security levels. Default value is **Auto Normal.**

6.2.4. Image Quality

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

6.2.5. Sensitivity

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.

6.2.6. Scan Timeout

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

6.2.7. Matching Timeout

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

6.2.8. 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 in normal mode. In typical cases, Fast Mode 1 is as 2 ~ 3 times faster than Normal mode. And Fast Mode 5 is 6 ~ 7 times faster than Normal mode.

6.2.9. Factory defaults of parameters

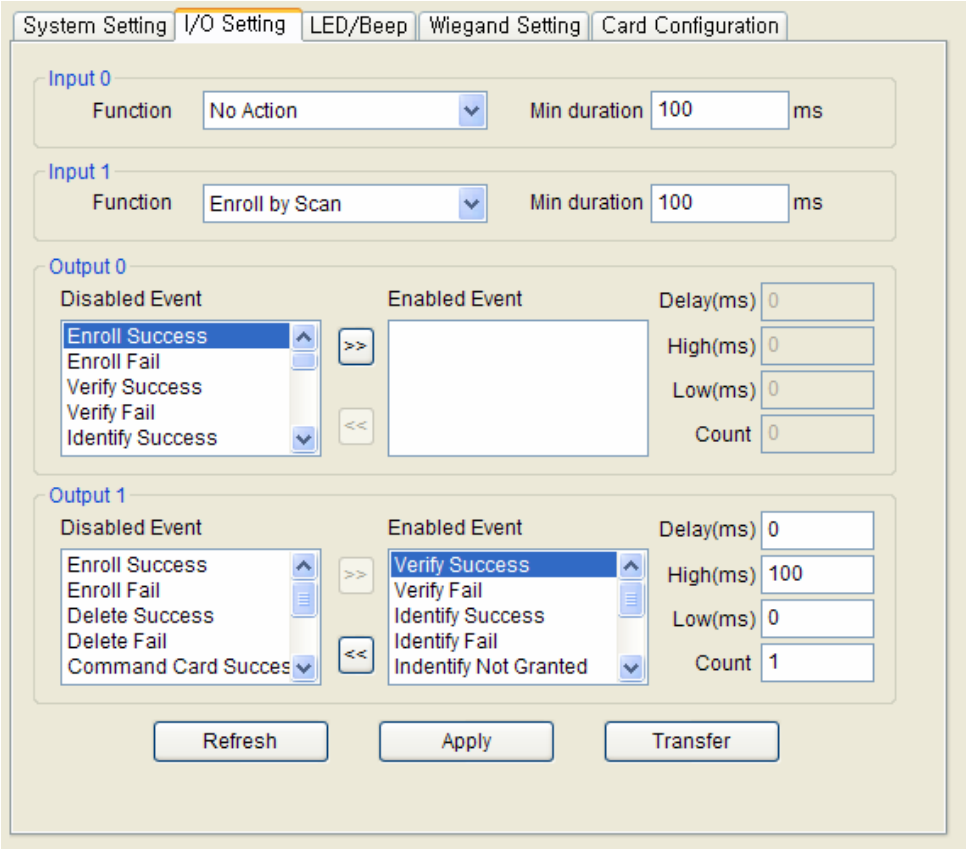
Factory defaults list of parameters for BioEntry™ Smart and BioEntry™ Pass is as follows :

	Factory defaults	Selectable values
Operation mode	1:1 verification (BioEntry™ Smart) 1:N verification (BioEntry™ Pass)	1:1 verification 1:N identification Both
Security level	Auto Normal	1/1,000 3/10,000 1/10,000 3/100,000 1/100,000 3/1,000,000 1/1,000,000 3/10,000,000 1/10,000,000 3/100,000,000 1/100,000,000 Auto Normal Auto Secure Auto More Secure
Image quality	Moderate	Weak Moderate

		Stronger Strongest
Sensitivity	7	0(lowest) to 7(highest)
Scan timeout	10 sec	1 to 20 sec or Infinite
Matching timeout	Infinite	1 to 20 sec or Infinite
Fast mode	0(Normal)	0(Normal) to 5(Fastest)

6.3. I/O Setting

BioEntry™ provides 2 programmable inputs and 2 programmable outputs which can be used to interface with external devices. **I/O Control** menu refreshes the main window to manage the I/O settings. By factory default, no functions are defined for each programmable I/O's.



6.3.1. Configuration of input port

To define the configuration of input port, function and minimum duration should be specified. Function means what to do when the input port is activated and minimum duration means the required duration of pulse to activate the input port.

6.3.2. Description of input functions

Function	Description
No Action	disable input port
Enroll by Scan	initiate enrollment using finger scan
Identify by Scan	initiate identification using finger scan
Delete by Scan	delete user by identifying input finger
Delete All	delete all user data
Enroll by Wiegand ID	enroll by scan with user ID received at Wiegand input port
Verify by Wiegand ID	initiate verification using finger scan with user ID received at Wiegand input port
Delete by Wiegand ID	delete user with user ID received at Wiegand input port
Controller Reject	input for reject signal from controller
Controller Accept	input for accept signal from controller
Software Reset	initiate software reset

6.3.3. Programming example for input port

If you want to connect an input button to initiate enrollment using user ID from Wiegand input, the following procedure is required. Let us assume that input port 0 is used and the button should be pressed at least 500 ms to activate the function.

- First, select a target reader on the device tree window.
- Select function of input port 0 as **Enroll by Wiegand ID**.
- Edit **Min duration** of input port 0 as 500.
- Press **Apply** button to transmit the new configuration to the target reader.

6.3.4. Configuration of output port

In configuring output port, multiple functions can be programmed to produce different output pattern on each event. Event means when to activate the output port and output pattern defines how to activate the output port, respectively. Programming procedure is as follows:

- Enable required event by selecting event from disabled event.

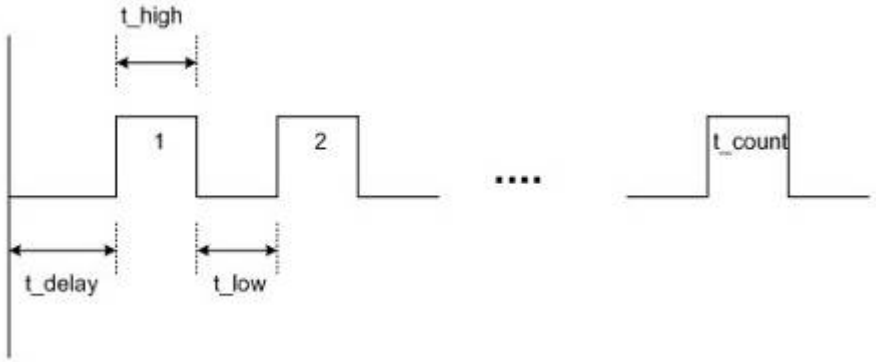
- Program output pattern by editing delay, high, low, and count values.

6.3.5. Description of output event

Event	Description (when to activate the output port)
Enroll Success	When a user is successfully enrolled on the reader
Enroll Fail	When enrollment fails
Identify Success	When identification is successfully done
Identify Fail	When the reader fails to find out the matched user
Verify Success	When verification is successfully done
Verify Fail	When the user is not verified
Delete Success	When deletion of user succeeds
Identify Not Granted	Identification is successfully done, but entrance denied
Verify Not Granted	Verification is successfully done, but entrance denied
Delete Fail	When deletion of user fails
Verify Duress	When duress finger is verified
Identify Duress	When identified finger is a duress finger
Temper Switch On	When temper switch on the reader is enabled implying reader is opened.
Command Card Success	When command card operation successfully completed
Command Card Fail	When command card operation is failed
Controller Reject	When input port on which Controller Reject function is assigned, is activated
Controller Accept	When input port on which Controller Accept function is assigned, is activated
Detect Input 0	When input port 0 is activated regardless of assigned function
Detect Input 1	When input port 1 is activated regardless of assigned function

6.3.6. Describing output pattern

On each enabled event, output pattern can be flexibly described by programming using 4 parameters whose meanings are depicted as



Parameter	Meaning	Allowed value
Delay	initial delay before generating output pulses in msec	0 ~ 65535
High duration	duration of pulse in high state in msec	0 ~ 65534 65535 : continuously active until new output event occurs
Low duration	interval between consecutive pulses where the output signal remains low	0 ~ 65535
Count	Number of pulses	0 : infinitely repeated until new output event occurs 1 ~ 255

6.3.7. Programming example of output pattern

Assume that a user want to assign an alarm signal at output port 0 generating following patterns:

- On identification success or verification success for duress finger, the reader sends blinking output during 5 seconds.
- When temper switch is on, the reader sends steady output during 10 seconds.

Programming procedure is as follows:

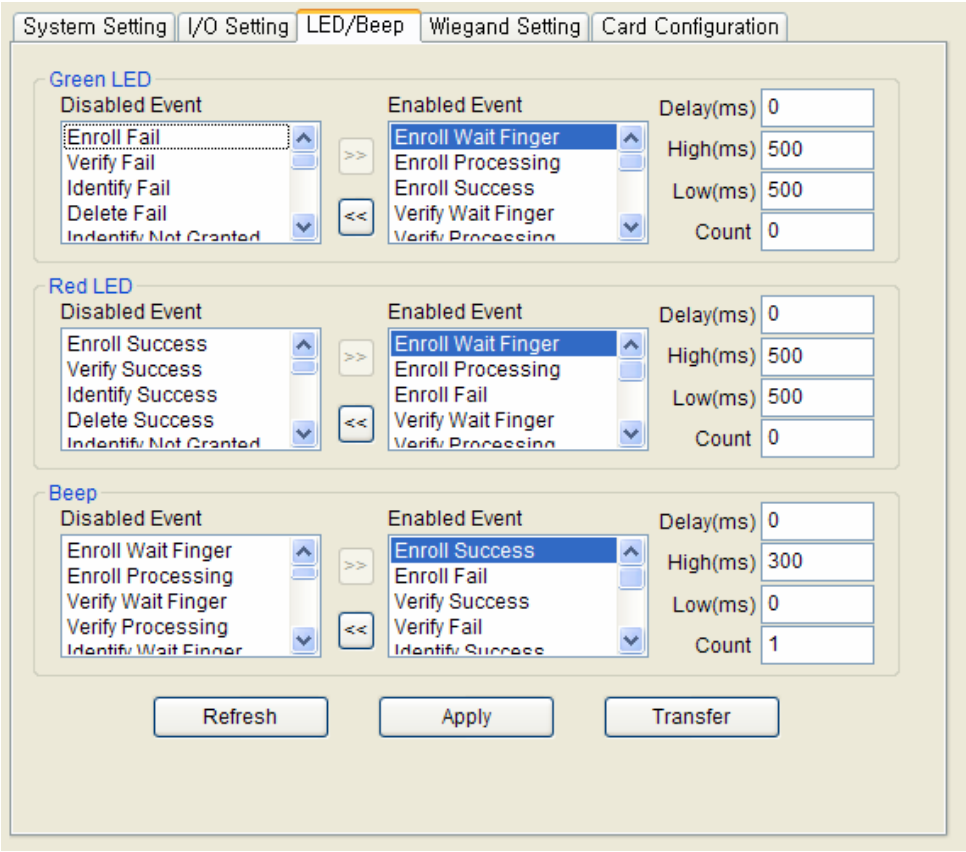
- First, select a target reader on the network window.
- Disable currently selected events on output 0 by moving enabled ones to the disabled sector.
- Program the required events by enabling each event followed by editing output pattern parameters as follows:

Event to be enabled	Output pattern parameters
Verify Duress	Delay : 0 High : 500 Low : 500 Count : 5
Identify Duress	Delay : 0 High : 500 Low : 500 Count : 5
Temper Switch On	Delay : 0 High : 10000 Low : 0 Count : 1

- Press the **Apply** button to transmit the new configuration to the target reader.

6.4. LED/Beep Setting

There are two LED's and one beep on BioEntry™ reader to provide processing status and result to users. The colors of two LED's are mixed to generate 3 colors, green, red, and amber. The configuration of LED and beep is similar to the output configuration described on Chapter 6.4.오류! 참조 원본을 찾을 수 없습니다.. 오류! 참조 원본을 찾을 수 없습니다.. By selecting the **LED/Beep Setting** tab, the LED/Beep configuration page is updated on the main window.



6.4.1. Configuration of LED/Beep

Programming steps for LED and Beep is similar to output port configuration. Please refer to Section 오류! 참조 원본을 찾을 수 없습니다.. 오류! 참조 원본을 찾을 수 없습니다.. For LED and Beep additional events are selectable, listed as

Event	Description (when to activate the output port)
Enroll Wait Finger	When the reader is waiting for a finger scan to enroll

Enroll Processing	When the reader is in enrollment process
Identify Wait Finger	When the reader is waiting for a finger scan to identify
Identify Processing	When the reader is in identification process
Verify Wait Finger	When the reader is waiting for a finger scan to verify
Verify Processing	When the reader is in verification process
Delete Wait Finger	When the reader is waiting for a finger scan to delete

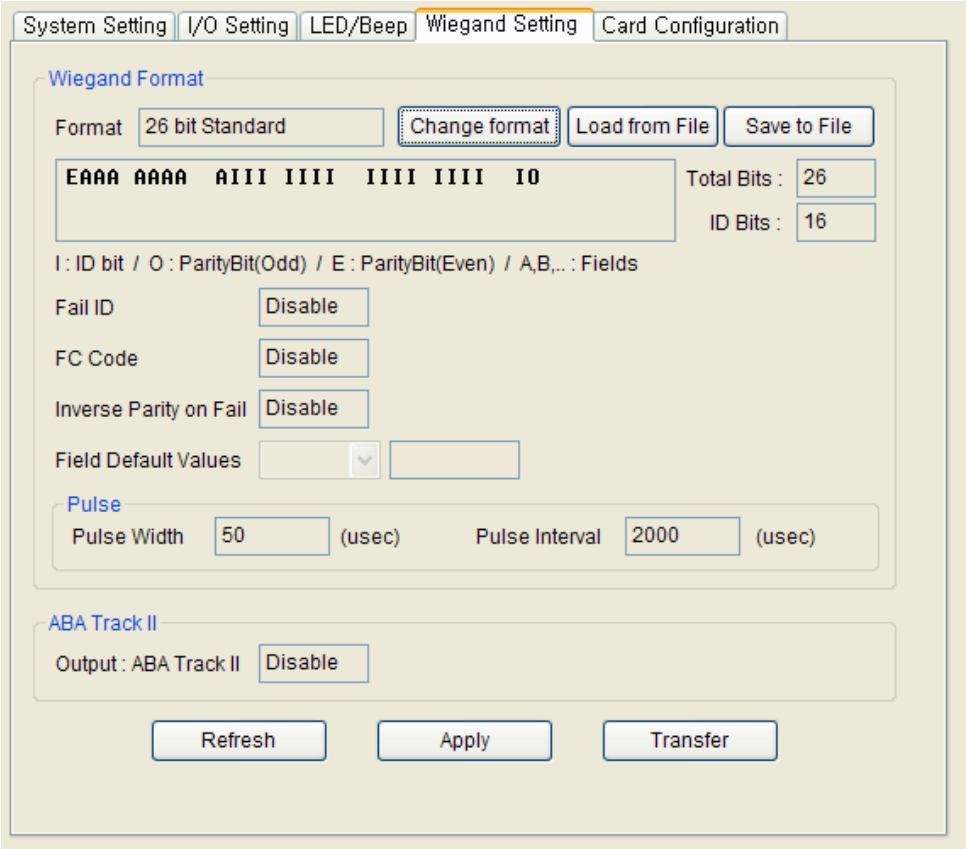
6.4.2. Description of default LED/Beep configuration

By factory default, various output patterns are defined for LED and beep to show current status and processing result. The description of default LED/Beep configuration is listed as follows:

Events	LED	Beep
Enroll Wait Finger	Slow blinking amber	None
Verify Wait Finger	Fast blinking amber	None
Identify Wait Finger	Slow blinking amber	None
Delete Wait Finger	Fast blinking amber	None
Enroll Processing Identify Processing Verify Processing	Steady amber	None
Enroll Success Verify Success Identify Success Delete Success Command Card Success Verify Duress Identify Duress	Steady green	One beep sound
Enroll Fail Verify Fail Identify Fail Delete Fail Command Card Fail	Steady red	Three short beep sounds
Waiting Smart Card Input	Fast blinking red (fixed)	None

6.5. Wiegand Setting

The **Wiegand Setting** tab is used to manage the Wiegand input/output format of BioEntry™. By selecting the menu, the Wiegand setting page is updated on the main window.



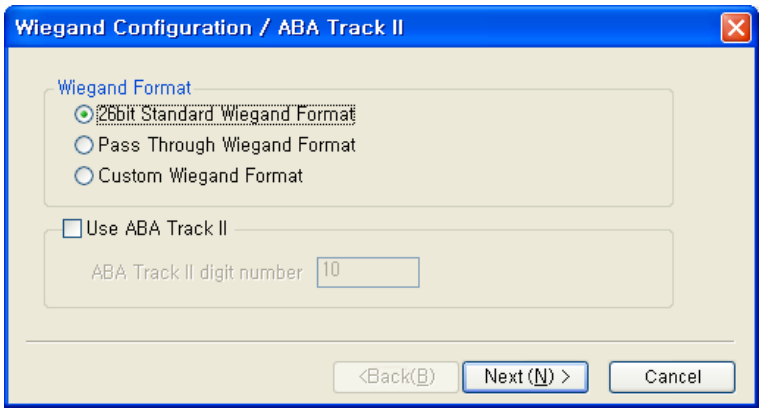
6.5.1. Editing new Wiegand configuration

New Wiegand format can be configured graphically using the Wiegand Configuration wizard. The Wiegand Configuration wizard will be shown by pressing the **Change format** button.

- Select format

You should select one of the three supported formats in the first page. If BioEntry reader is connected to the controller by ABA Track II output, not by Wiegand interface, you should check **Use ABA Track II**. In that case, the output signal will be in ABA Track II format. You can also specify the number of characters for ABA

Track II output.



- 26 bit standard

The 26 bit standard format is most widely used and consists of 8 bit FC code and 16 bit ID. You cannot change the bit definition and the parity bits in 26 bit standard format.

- Pass Through format

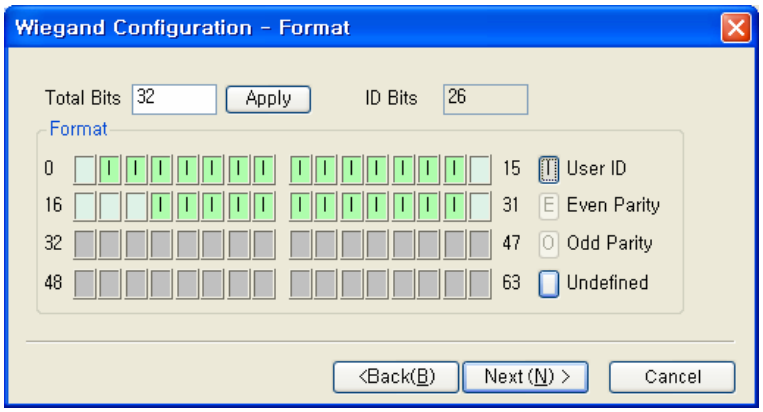
Pass Through format is used when only the format of ID field is known. When the Wiegand input string is detected, BioEntry reader extracts ID bits and starts verification with the ID. If the verification succeeds, the reader outputs the Wiegand input string as unchanged. Parity check and advanced options are ignored in this format. By definition, Pass Through format is only useful when the operation mode is 1:1. If the mode is 1:N, the bits other than ID field are set to 0.

For example, assume that 32 bit Pass Through format is composed as follows:

`XIIIIIII IIIIIIIX XXXIIIII IIIIIIIX` (left most bit is 0th bit, BIT0)

I: Id field, X: Unknown field

You can configure this format in the following sequences.



(1) Enter 32 in the **Total Bits** field.

(2) Select ID bits according to the definitions.

(3) Press **Next**. You cannot specify parity bits in Pass Through mode.

6.5.2. Custom format

When users know all the information of a Wiegand format, Custom format can be defined. When a Wiegand input string is detected, BioEntry reader checks the parity bits first. If all the parity bits are correct, the reader 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 reader outputs a Wiegand string. The output string may be different from the input string according to the alternative values and advanced options.

For example, assume that 44 bit Custom format is composed as follows:

`EAAAAAAA IIIIIIII IIIIIIII BBBBBBBI IIIIIIII III0`

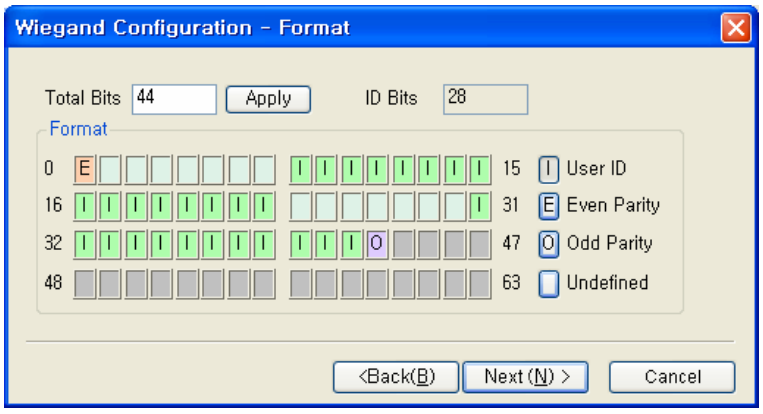
(left most bit is 0th bit, BIT0)

E: Even parity for BIT1 ~ BIT22

O: Odd parity for BIT23 ~ BIT42

I: ID bits(Field1 and Field 3), A: Field 0, B: Field 2

You can configure this format in the following sequences.



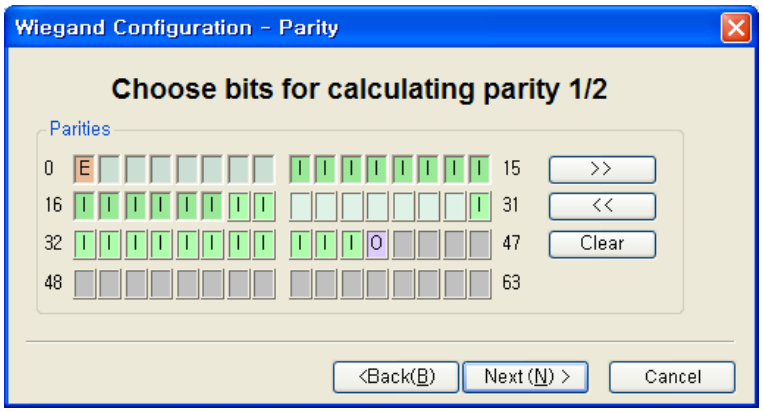
(1) Enter 44 in the **Total Bits** field.

(2) Select **Even Parity**.

(3) Press the even parity bit. In this example, it is BIT0.

(4) Repeat (2) and (3) for **Odd Parity** and **User ID** according to the definition.

(5) Press **Next**.



(6) Press the bits which are used in calculating the first parity bit. In this example, they are BIT1 ~ BIT22

(7) Press **>>**.

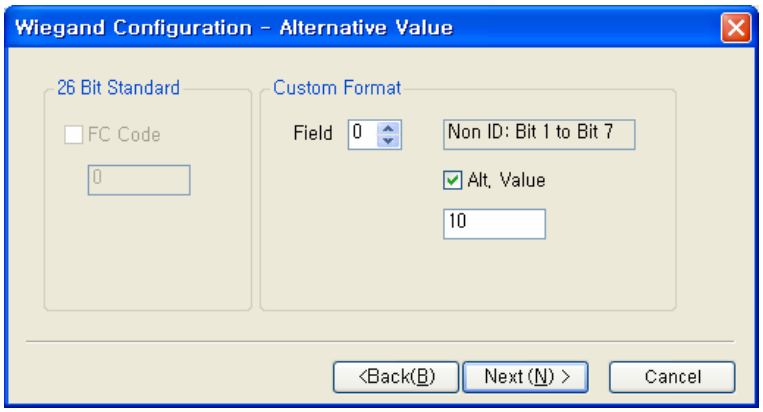
(8) Press the bits which are used in calculating the second parity bit. In this example, they are BIT23~ BIT42.

(9) Press **Next**.

6.5.3. Alternative values

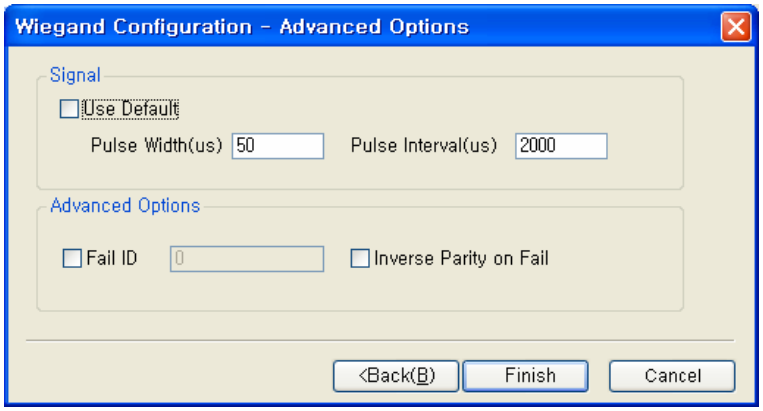
In 26 bit standard you can specify alternative FC code. In Custom format, you can specify alternative values for non-ID field. If alternative values are set, the

BioEntry™ reader will replace corresponding fields with these values before sending outputs.



6.5.4. Advanced options

You can specify the characteristics of Wiegand signal and the advanced options in the last page of the wizard. Advanced options are not available for Pass Through format.

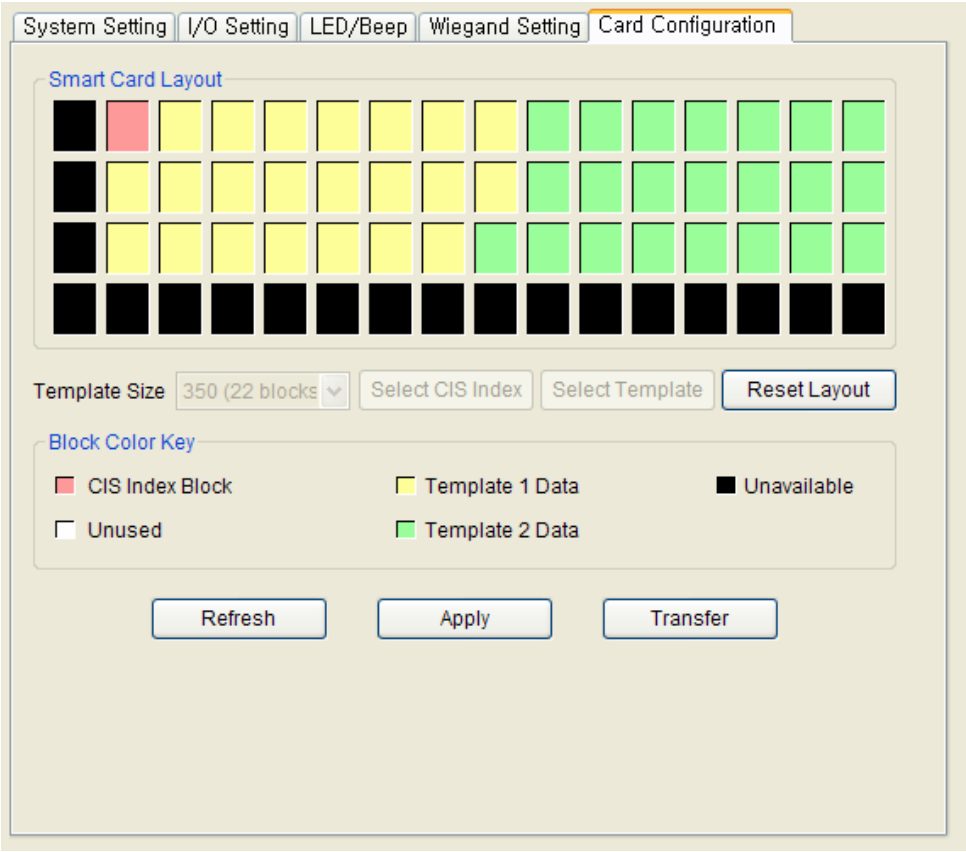


- **Use Default**: Uses default values for Wiegand signals.
- **Pulse Width**: The width of pulse. The default is 50 us.
- **Pulse Interval**: The interval of pulse. The default is 2000us.

- **Fail ID**: Normally the module outputs Wiegand signals only if matching succeeds. If this option is checked, the module outputs the fail ID when matching fails.
- **Inverse Parity on Fail**: If this option is checked, the module outputs Wiegand signals with inverted parities when matching fails.

6.6. Card Configuration

Card Configuration is the process of defining custom sectors on user's smart card to store user information including user ID and templates. By selecting **Card Configuration** menu, smart card layout page is updated on the main window. ***It is recommended that only advanced users attempt to change the layout since improper changes may render the smart card unusable. Read this chapter carefully for changing the layout from the default configuration.***



6.6.1. Editing layout

- Template size

Template size is configurable from 254 to 382. By factory default, template size is specified as 350 bytes storing two templates on the card.

- CIS index block : Header information is stored on the CIS index block which is depicted by red color.
- Template data block : Blocks for template 1 data and template 2 data. Number of blocks for each template data is determined by template size. Template 1

data is depicted by yellow and template 2 data is depicted by green, respectively.

- Unused block : Blank block which is not defined by layout.
- Unavailable block : Block that is prohibited from use.

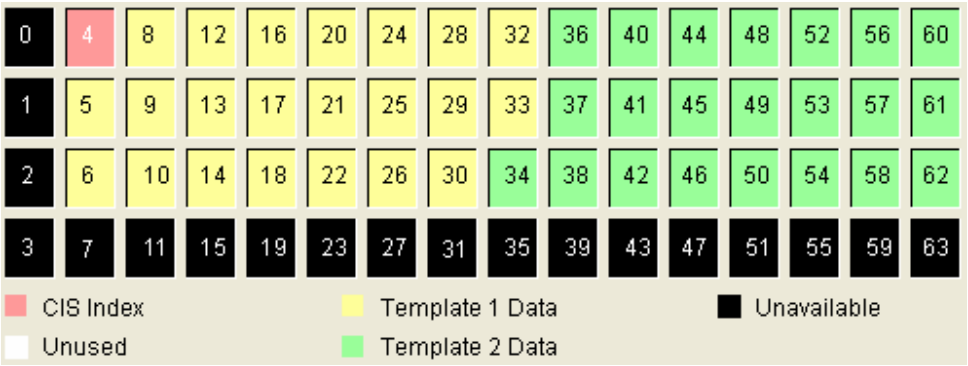
6.6.2. Editing procedure

To configure customer's layout, following procedures are required.

- Initialize all the blocks to unused ones by pressing the **Reset Layout** button.
- Select the required template size.
- Press the **Select CIS Index** button and click an unused block to select a CIS index block.
- Press the **Select Template** button and click an unused block to indicate the start block of template data. Then, the blocks of template 1 data are set automatically from the selected start block.
- Press the **Select Template** button again and click an unused block to indicate the start block of template 2 data.
- The **Apply** button transmits smart card layout to selected readers**.**

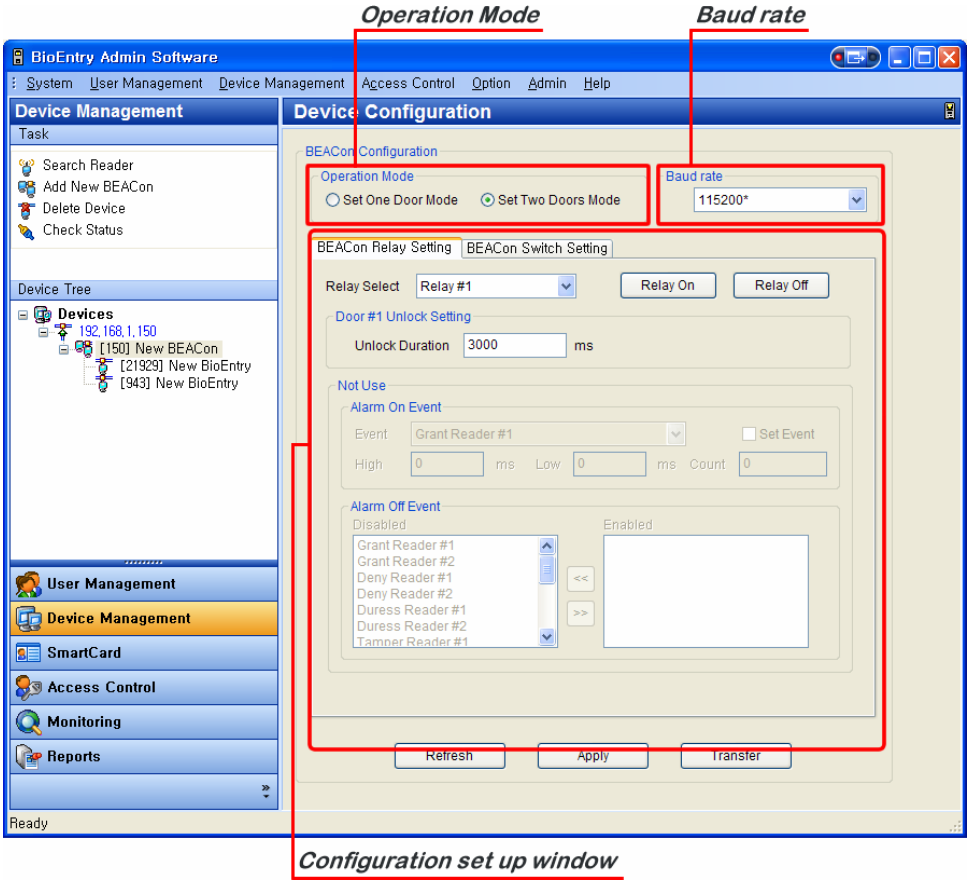
6.6.3. Factory default layout

Factory default smart card layout is as follows :



6.7. BEACon™ Configuration

By selecting a BEACon™ on the Device tree, the Device Configuration window for the selected BEACon™ is updated on the main window.



The Device Configuration window is divided into 3 sectors:

- Operation Mode

BEACon™ can control up to two doors. The Operation Mode window shows whether the selected BEACon™ is configured as one door mode or two door mode.

- Baud Rate

The Baud rate window shows the transmission speed of the selected BEACon™.

- Configuration Set up window

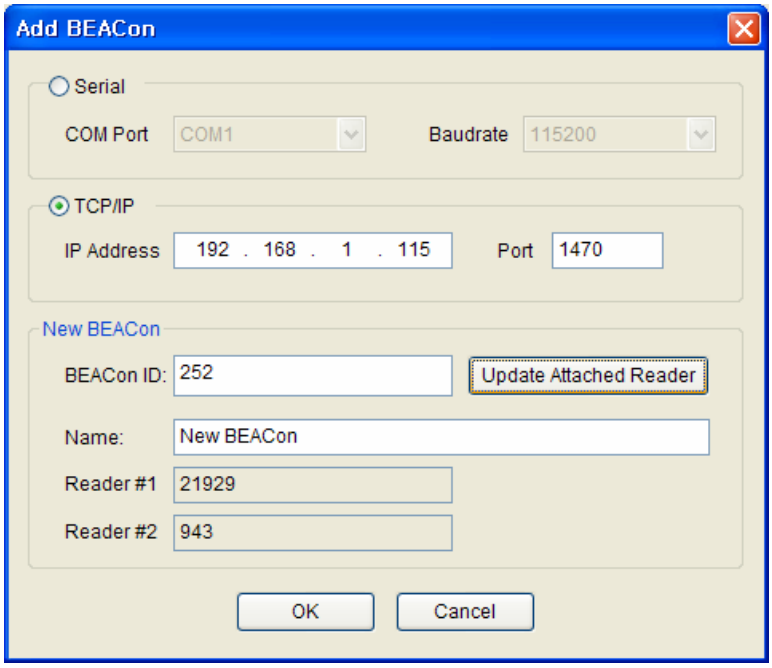
The Configuration set up window shows the current configurations of the selected BEACon™. Also, this window shows the configurations to be changed. The

configuration set up menus are divided by separate tabs, such as BEACon Relay Setting and BEACon Switch Setting.

**** For the detailed operation of BEACon™, refer to BEACon™ operation manual.**

6.7.1. Add New BEACon™

To network BEACon™ with a host PC, you need to designate the ID or IP(for Ethernet interface only) on BEACon™. (For the detailed operation of ID/IP setting, refer to BEACon™ operation manual.) Upon adding a new BEACon™, this designated ID/IP needs to be entered again on the BioAdmin



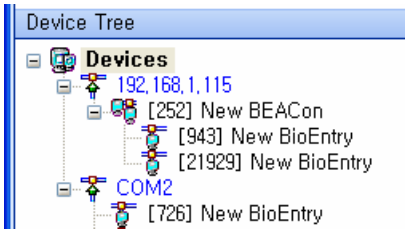
Detailed operations are as follows.

- Press the **Add New BEACon** button on the task box.
- Select the communication method between Serial and TCP/IP.
- Enter the BEACon™ ID, which you previously entered on the BEACon™.

(For the ID setting of BEACon™, refer to ID setting on the BEACon™ operation manual.)

- Press the **Update Attached Reader** button.

- Attached reader will be shown on **Reader #1** / **Reader #2.**
- Press the **OK** button.



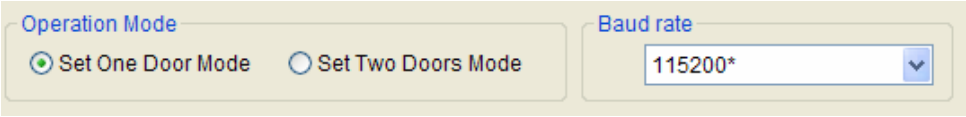
6.7.2. Operation Mode & Baud rate

BEACon™ can control up to two doors. The Operation Mode window shows whether the selected BEACon™ is configured as one door mode or two door mode.

- Operation Mode (OP Mode): BEACon™ can control up to two doors. You can select the operation mode depending on your application.

The Baud rate window shows the transmission speed of the selected BEACon™.

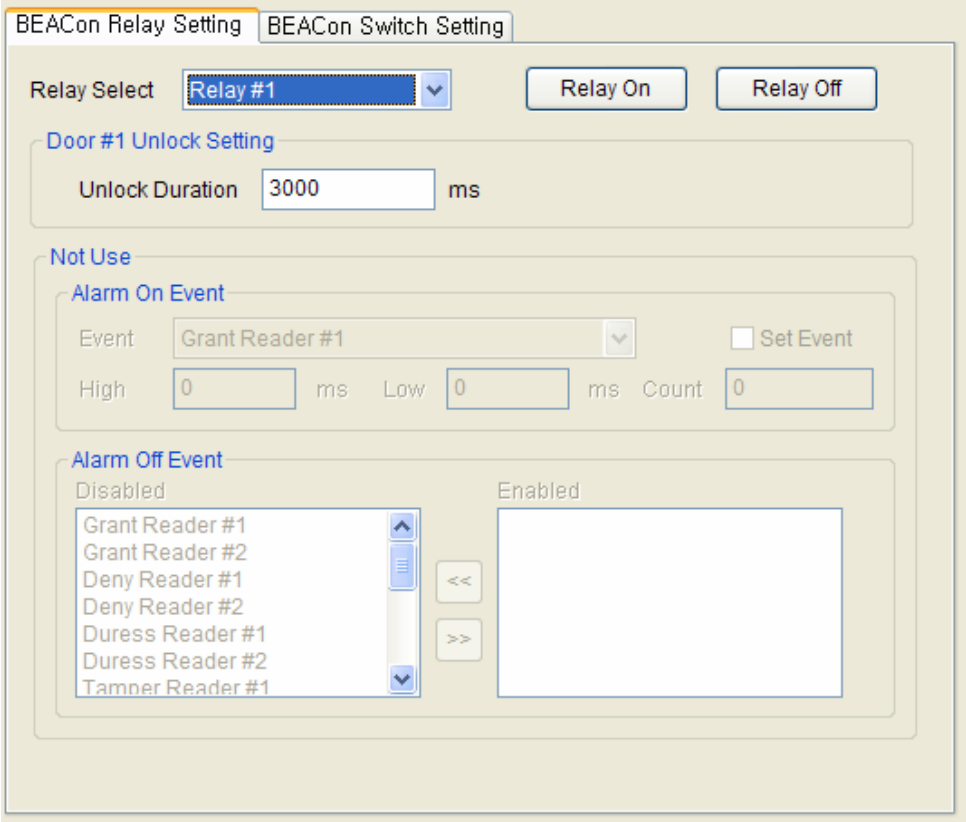
- Baud rate: On this menu, you can select the transmission speed of BEACon™. If you change the Baud rate on this menu, communication speed between BEACon™ and host PC will be changed.
- Once you change the Baud rate of BEACon™, you also need to accord the Baud rate of BioEntry™ with the changed Baud rate of BEACon™.



6.7.3. BEACon™ Relay Setting

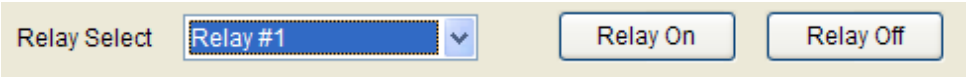
On this menu, you can change the relay setting of BEACon™. The relay setting can be differently configured depending on the operation mode of BEACon™.

- On 1 door mode, relay #1 is automatically set up as door release. Therefore, you can set up relay #2, #3, and #4 as alarm.
- On 2 door mode, relay #1 and #2 are automatically set up as door release. Therefore, you can set up relay #3 and #4 as alarm.



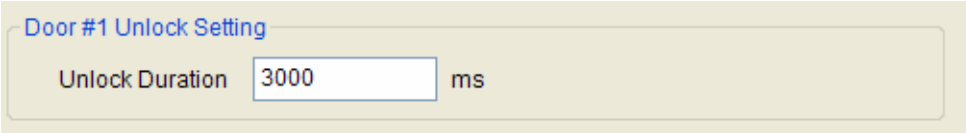
Detailed Operations are as follows.

- Select a relay to set up the configuration. Once you select a relay, applicable items for the selected relay will be activated on the relay setting window.
- You can also open/close the relays by pressing the **Relay On** / **Relay Off** buttons.



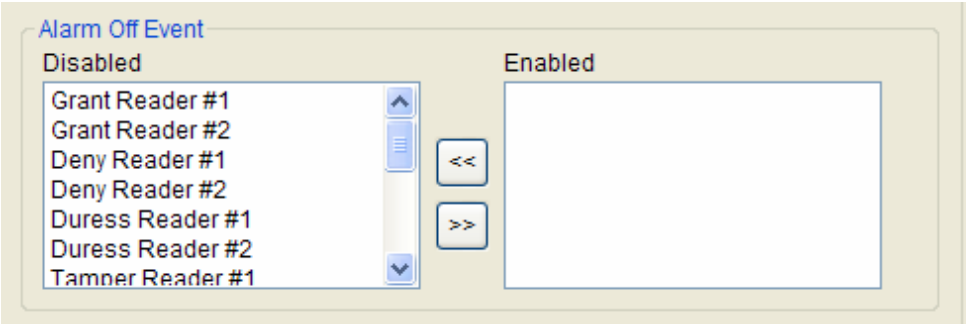
- Unlock Setting

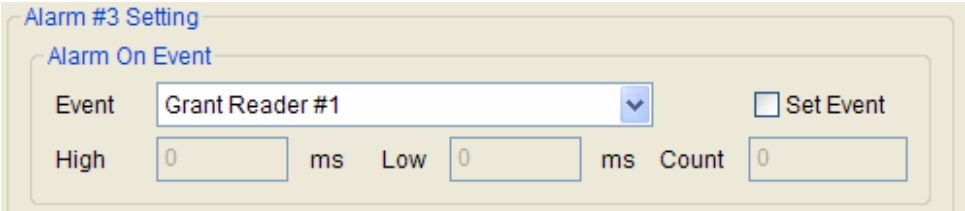
Enter the unlock duration time. Once the door is unlocked, it can be locked again after this unlock duration time.



- **Alarm On Event**:

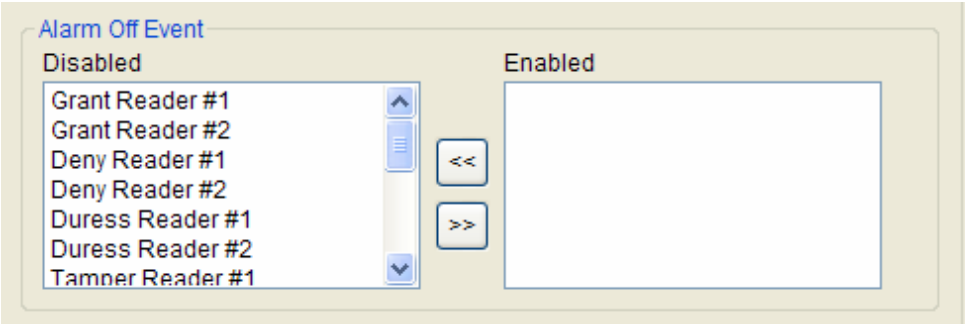
Select alarm on events on the drag down menu by checking on the **Set Event** check box. Enter **High**, **Low**, and **Count** to set up the alarm frequency. If any of the alarm on events is triggered, the alarm will be activated at your designated frequency.





- **Alarm Off Event**:

Select alarm off events. You can enable the alarm off events simply by double clicking the events on the disabled event list. If any of the alarm off events is triggered, the alarm will be deactivated, regardless of remaining duration or pulse counts.

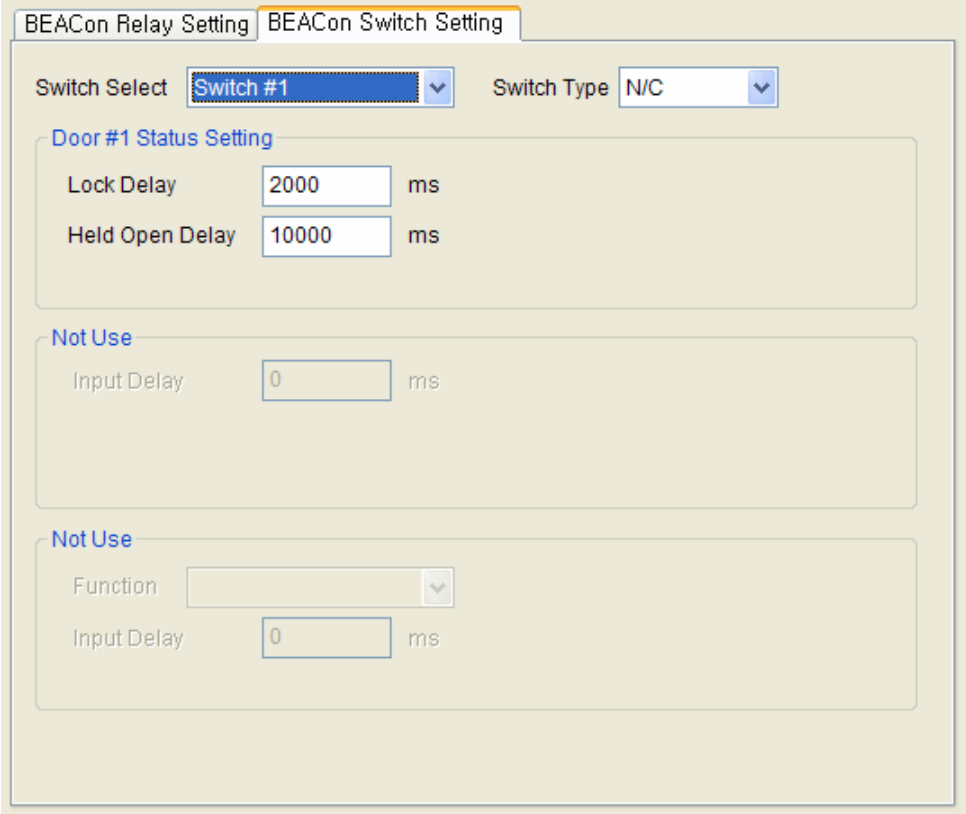


6.7.4. BEACon™ Switch Setting

On this menu, you can change the switch setting of BEACon™. The switch setting can be differently configured depending on the operation mode of

BEACon™.

- On 1 door mode, switch #1 is automatically set up as the door sensor and #3 as RTE (request to exit). Therefore, you can set up switch #2, #4, #5, and #6 as other various functions on the Normal Switch Setting menu.
- On 2 door mode, switch #1 and #2 are automatically set up for the door sensor. Also, switch #3 and #4 are automatically set up for RTE. Therefore, you can set up switch #5 and #6 for other various functions on the Normal Switch Setting menu.



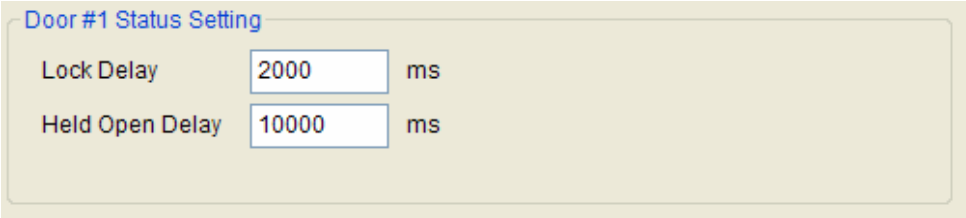
- Select a switch to set up the configuration. Once you select a switch, applicable items for the selected switch will be activated on the switch setting window.

- Door Status Setting

By selecting a door sensor switch, you can set up the lock delay and held open delay of the connected BEACon™.

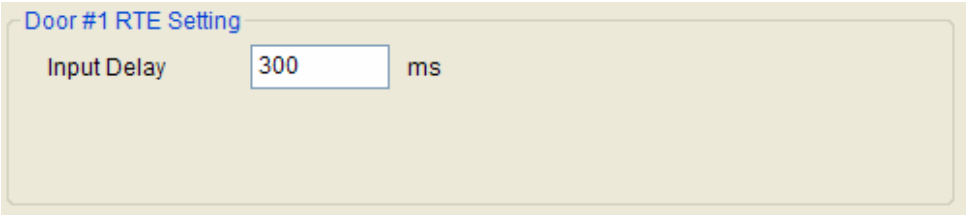
If the door is closed, the door strike will be locked after your designated lock delay time.

If the door is opened for more than your designated Held Open Delay time, the heldopen door event will be triggered.



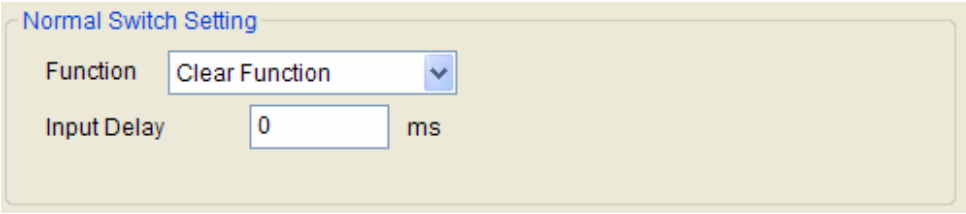
- Door RTE Setting

By selecting RTE switch, you can set up the input delay. If the RTE switch is activated for more than your designated input delay time, the door will be opened.



- Normal Switch Setting

For the remaining switches, you can set up other various functions, such as RTE, tamper, clear alarm switch. If the switch is activated for more than your designated input delay time, the selected function will be triggered.



6.7.5. Refresh / Apply / Transfer

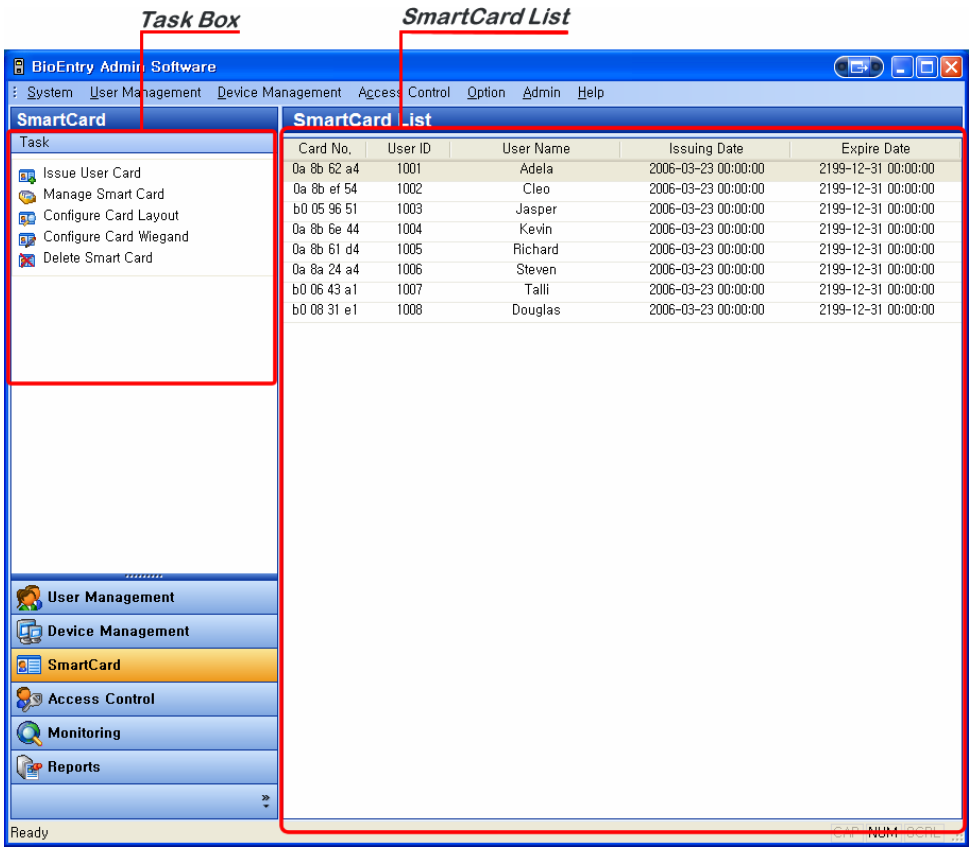
- Refresh : You can restore the original configuration by pressing the **Refresh** button before pressing Apply button.
- Apply : After changing the configuration, you need to press the **Apply** button to save.
- Transfer : You can transmit the changed configurations to other devices by pressing the **Transfer** button.

7. Smart Card

The Smart Card menu is used to see the list of smartcards issued on the BioAdmin Software. All of user's smart cards will be automatically shown on the SmartCard list of this menu.

The SmartCard menu covers the following operations:

- Issue User Card
- Manage Smartcard
- Configure Card Layout
- Configure Card Wiegand
- Delete Smartcard



7.1. Organization of Smartcard page

By selecting **Smart Card** menu, Smart Card management page is updated on the main window.

The SmartCard page is divided into 2 sectors:

- Smartcard List

The Smart card database is under central management on host PC. The Smartcard list includes the detailed list of smart cards issued on BioAdmin software.

- Task box

Task box includes buttons to control the basic operations of the SmartCard page.

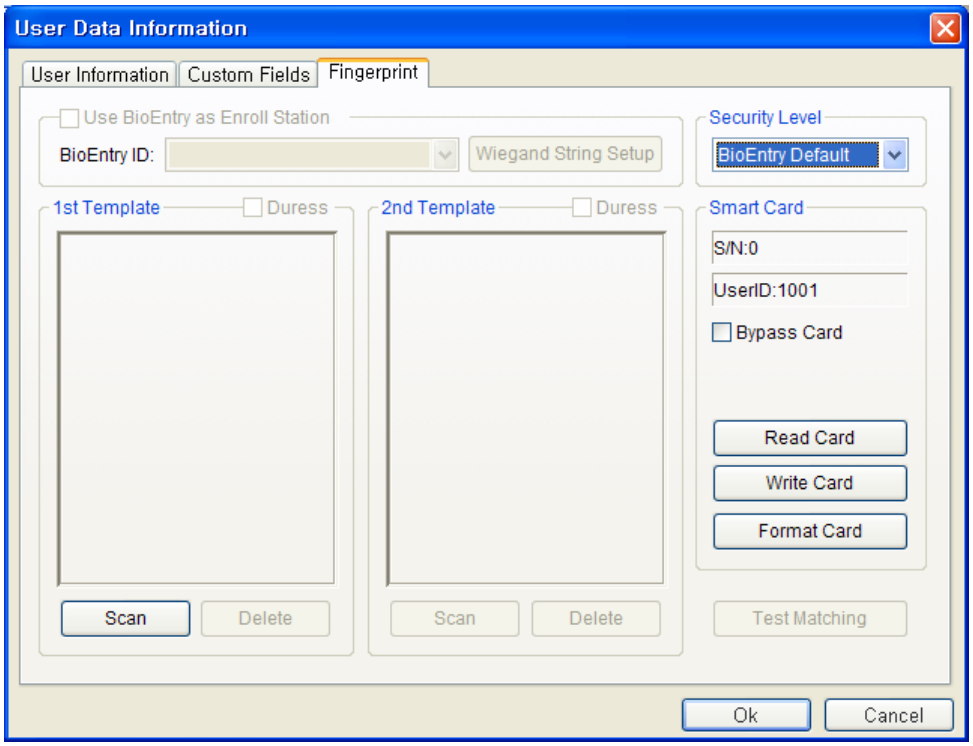
7.2. Smartcard List

The Smartcard list includes the following information of the Smartcards.

- Card Number
- User ID
- User Name
- Issuing Date
- Expiry Date

7.3. Issue User Card

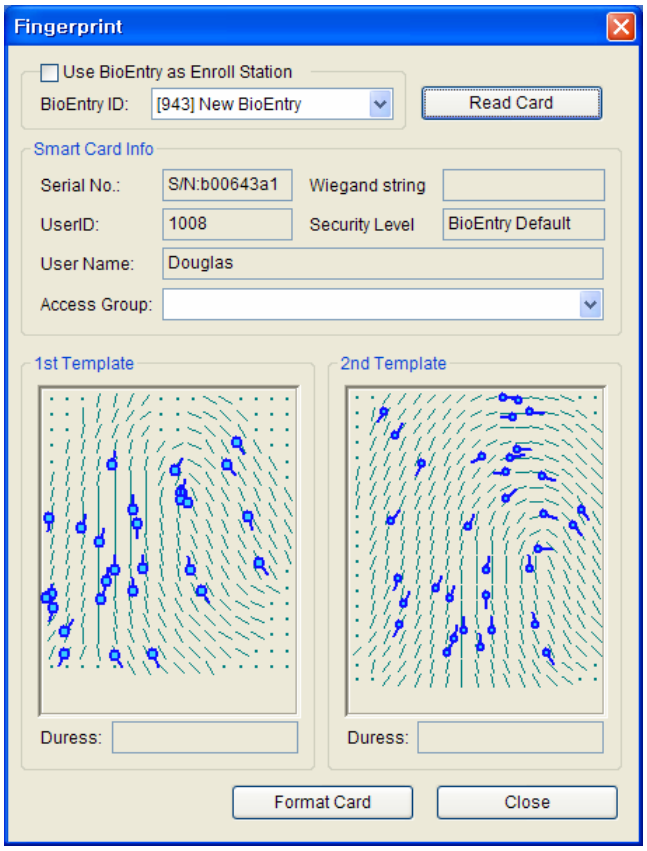
The **Issue User Card** menu enables a pop-up window to issue a user's smart card. For the detailed operation, refer to the issuing procedure on the User Management menu.



7.4. Manage Smartcard

The **Manage Smartcard** menu enables a pop-up window to read the smart card information and format smart card. On this window, you can check the smartcard information such as Serial No, Wiegand string(if applicable), User ID, Security Level, User Name, Access Group, and Template Data.

If you do not have a USB smart card Reader/Writer, you can also read the smart card information directly through BioEntry™ by check on **Use BioEntry as Enroll Station.**



7.4.1. Reading issued smart card

On this Manage Smartcard window, information stored on the smart card can be retrieved similarly to the reading process described in Chapter 5. User Management.

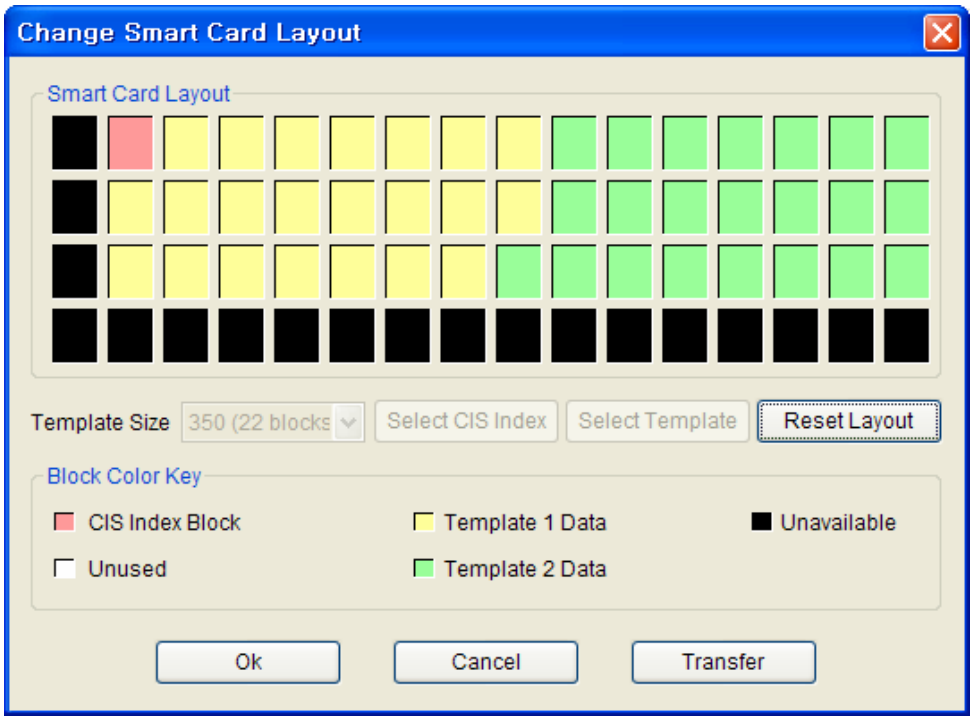
7.4.2. Formatting smart card

On this Manage Smartcard window, the formatting can be processed similarly to the formatting process described in Chapter 5. User Management.

7.5. Configure Card Layout

Smartcard layout is the process of defining custom sectors on user's smart card to store user information including templates. By selecting the **Configure Smartcard** button, the smartcard layout page is updated on the main window. ***It is recommended that only advanced users attempt to change the layout***

since improper changes may render the smart card unusable. Read this chapter carefully for changing the layout from the default configuration.



7.5.1. Organization of smartcard layout page

The Configure Smartcard layout page is divided into 3 sectors :

- Smart Card Layout

It shows the smartcard layout of the Smartcard Reader/Writer device connected to the host PC.

- Smart Card Layout

It shows the name of currently selected reader and the layout of the current reader. If a group or all readers are selected, the contents are not available.

- New configuration

This sector is used for editing new layout to be applied to the readers and the user's smart card.

- Controls for managing layout

Fill with Current Configuration Value button updates the contents of the new configuration using the retrieved layout from currently selected reader. **Transfer** button transmits new layout to the selected BioEntry™ reader, selected group, or

all BioEntry™ readers. Several control buttons for editing layout also exist.

7.5.2. Template size

Template size is configurable from 254 to 382. By factory default, template size is specified as 350 bytes storing two templates on the card.

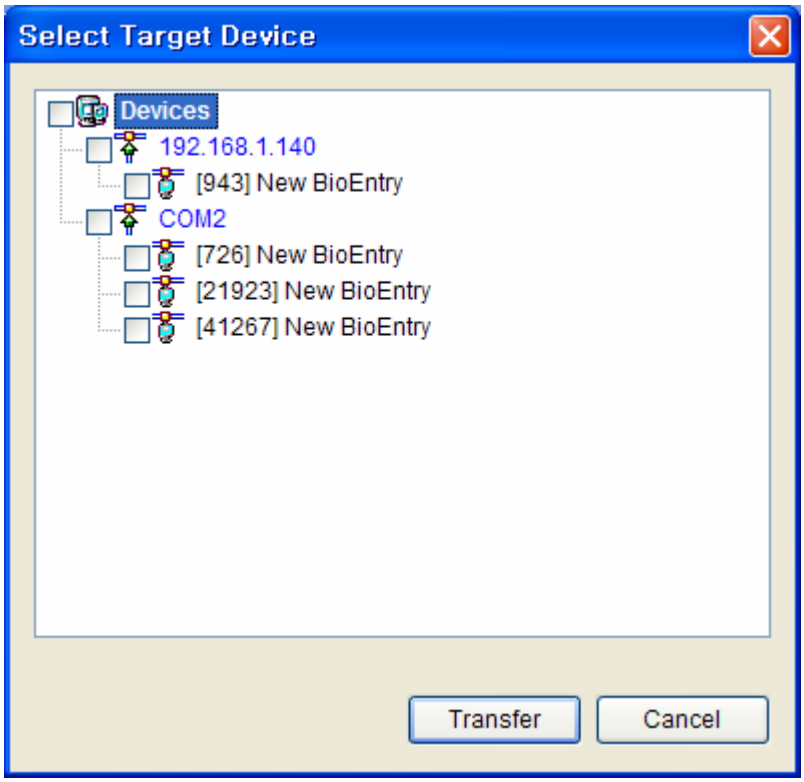
7.5.3. Blocks

- CIS index block : The header information is stored on the CIS index block which is depicted by red color.
- Template data block : Blocks for template 1 data and template 2 data. The number of blocks for each template data is determined by template size. Template 1 data is depicted by yellow and template 2 data is depicted by green, respectively.
- Unused block : Blank block which is not defined by layout.
- Unavailable block : Block that is prohibited from use.

7.5.4. Editing procedure

To configure customer's layout, the following procedure is required.

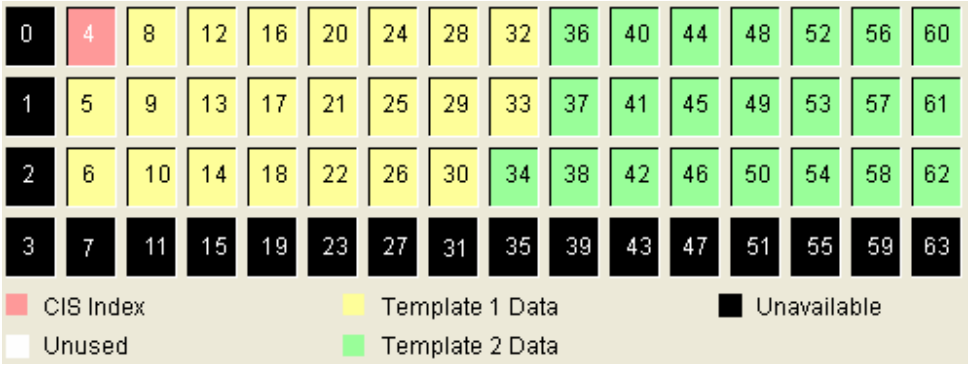
- Initialize all the blocks to unused ones by pressing the **Reset Layout** button.
- Select the required template size.
- Press the **Select CIS Index** button and click an unused block to select a CIS index block.
- Press the **Select Template** button and click an unused block to indicate the start block of template data. Then, the blocks of template 1 data are set automatically from the selected start block.
- Press the **Select Template** button again and click an unused block to indicate the start block of template 2 data.
- Press the **Transfer** button to transfer the new smart card layout to selected readers.



- The smart card layout window is activated only for BioEntry™ Smart model. If the selected device is BioEntry™ Pass, this menu will not be activated.
- Press the **OK** button to save the new smartcard layout to the PC USB smartcard reader/writer.
- The saved layout is also applied in issuing a new smartcard using PC USB smartcard reader/writer.

7.5.5. Factory default layout

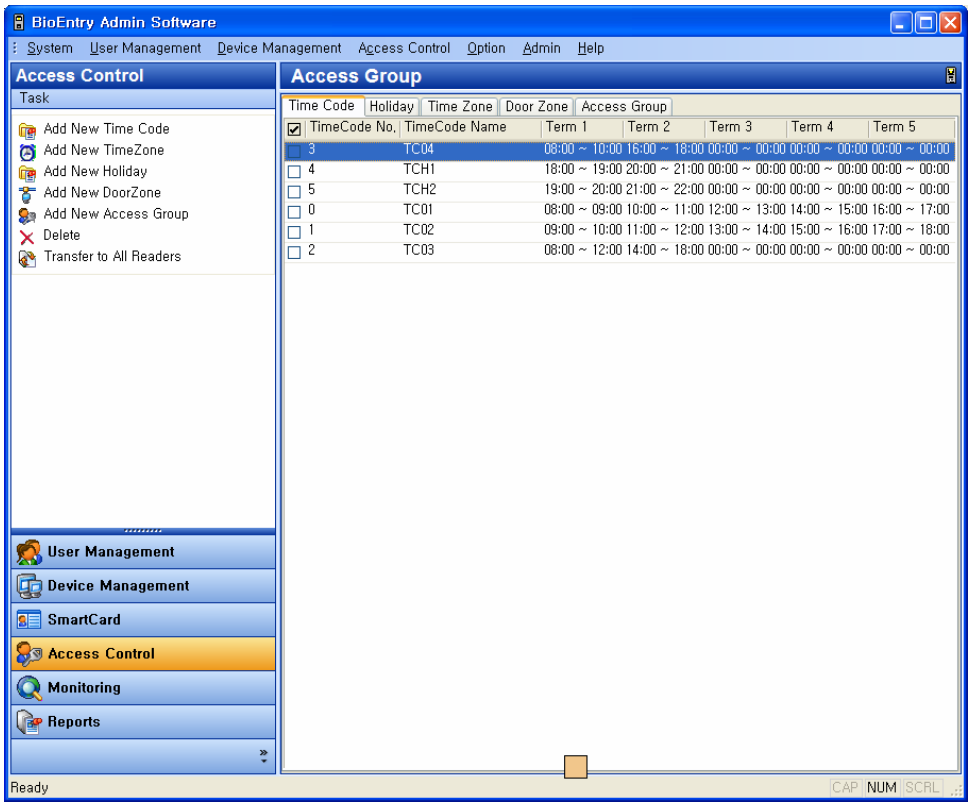
Factory default smart card layout is as follows :



8. Access Control

On this menu, you can set up the Time Zone and Access Group. Time Zone and Access Group are used to restrict user's right to access according to previously designated rules.

- If a user is not included in any access group, the user is allowed to enter every door.
- If a user is included in an access group, but a BioEntry™ reader does not have the access group information, the user is allowed to enter the door without restriction.

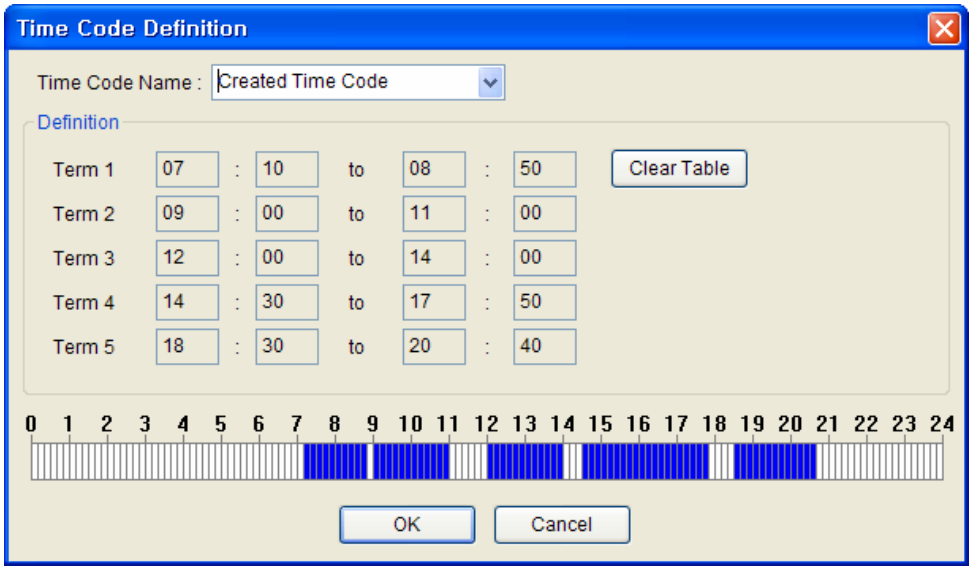


8.1. Time Code

You can set up Time Zone by combining several Time Codes. Therefore, before setting up the time zone, you need to set up the time code first. Maximum 5 time sections can be selected for each time code.

Detailed operations are as follows.

- Press the **Add New Time Code** button.



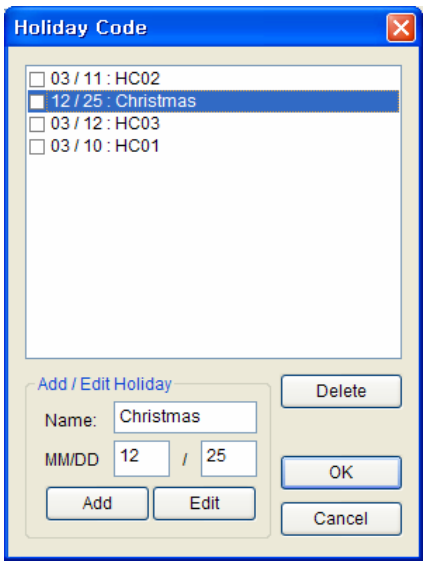
- Enter the name of time code.
- Set up the time code by entering time on the boxes.
- You can also set up the time code simply by dragging on the time bar on the bottom of time definition window.
- Press the **Ok** button to add the time code on time code list.

8.2. Holiday

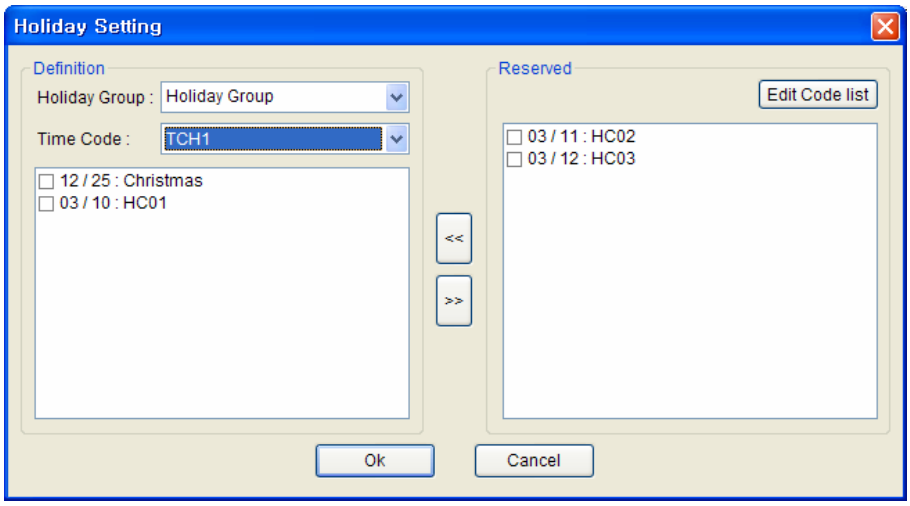
To include holidays on the Time Zone, you need to set up holidays in advance.

Detailed operations is as follows.

- Press the **Add New Holiday** button.
- Press the **Edit Code list** in **Holiday Setting** window.



- Add, edit or delete holiday code list, and press the **Ok** button.
- Enter the name of holiday group.
- Select Time Codes for the holiday.
- After checking on the Holiday Code, click **<<** button.

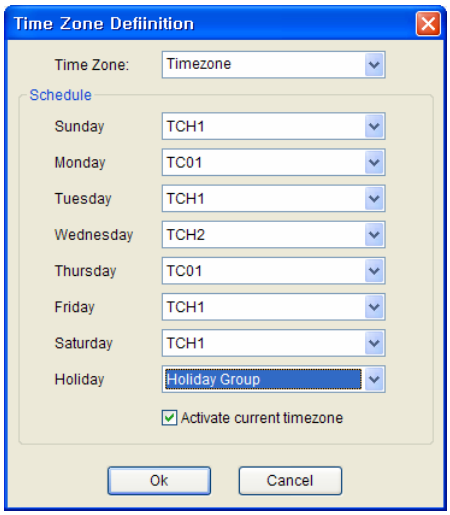


- Press **Ok** button to add the holiday on the holiday list.

8.3. Time Zone

You can set up a Time Zone by combining time codes and a holiday group. One time code is selected for each day from Monday to Sunday. Detailed operations are as follows.

- Press the **Add New Time Zone** button.
- Enter the name of the Time Zone.

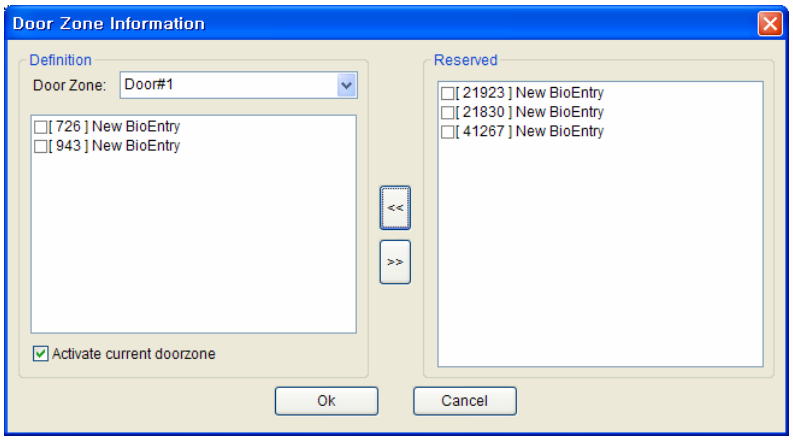


- Select a time code for each day from Monday to Sunday.
- Select a holyday group for the time zone.
- Press the **Ok** button to add the holiday group to the time zone list.

8.4. Door Zone

You can set up a door zone combining multiple BioEntry™ readers.

- Enter the name of the door zone.
- Check on the target BioEntry™ readers and click the **<<** button.

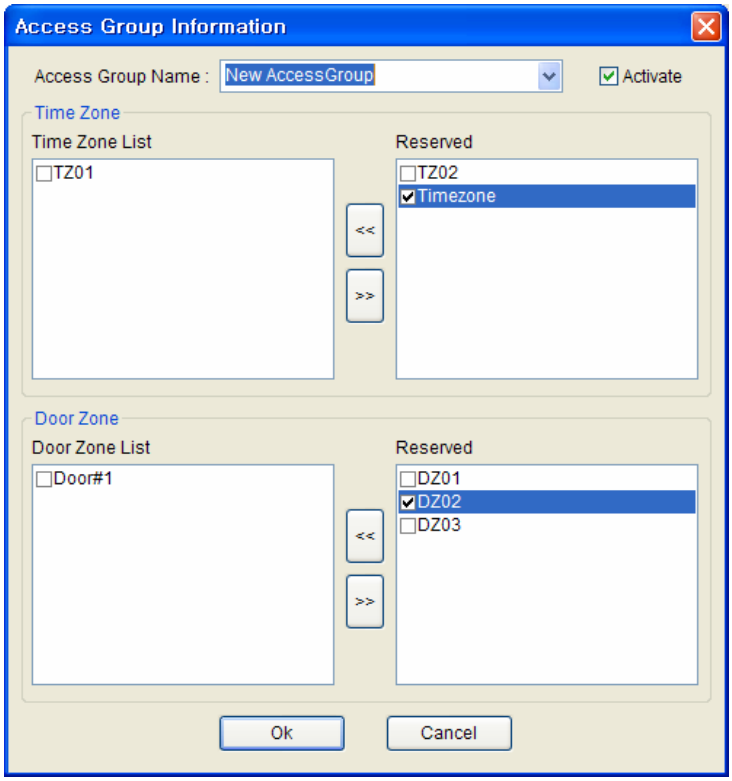


- Press the **Ok** button to add the door zone on the door zone list.

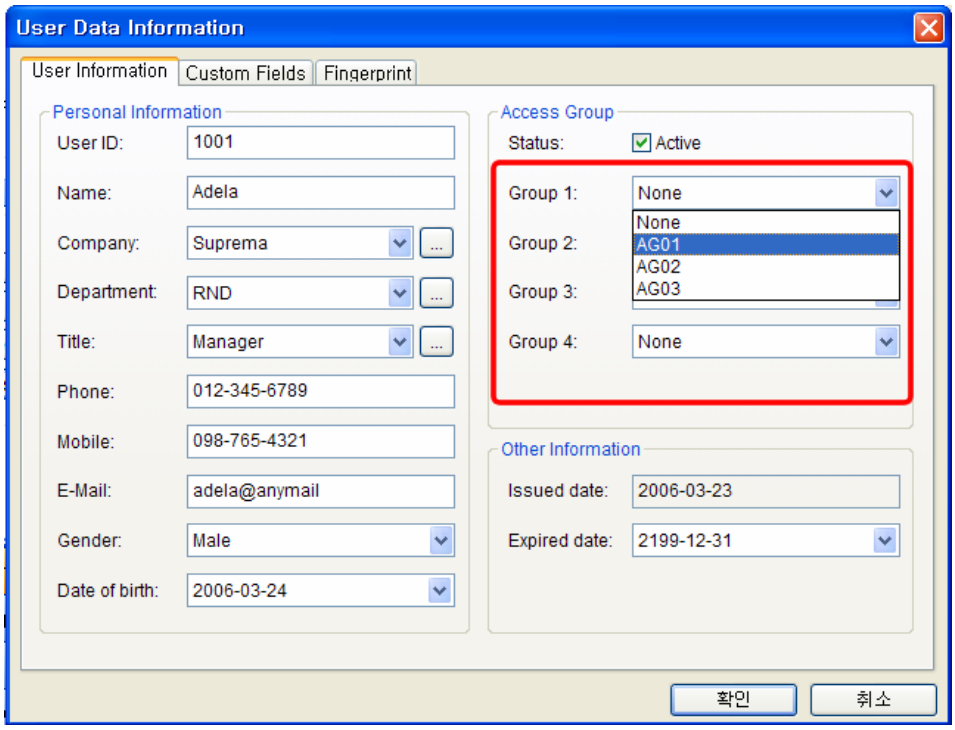
8.5. Access Group

By combining time zone and door zone, you can designate an access group. With this access group, you can restrict the user's right to access.

- Press the **Add New Access Group** button.
- Enter the name of access group.
- Check on the time zone and door zone and press the **<<** button.



- Press the **Ok** button to add the selected access group to the access group list. You can apply this access group to users on the **User Management** menu.

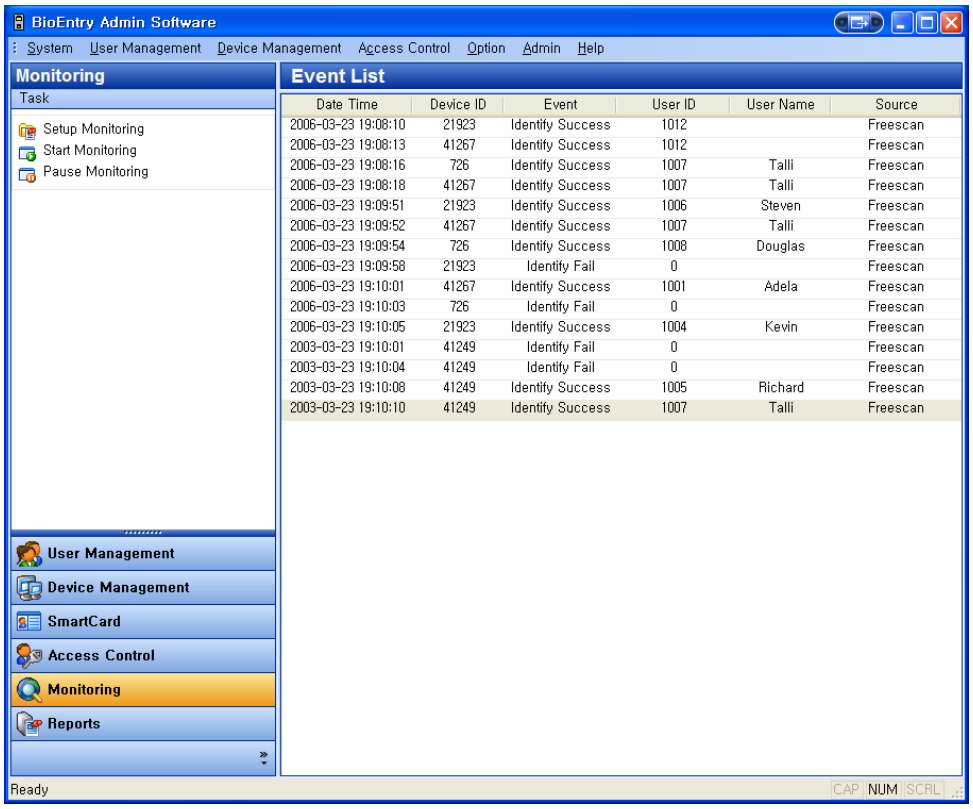


- For the detailed operation on User data, refer to Chapter 5. User Management menuu.

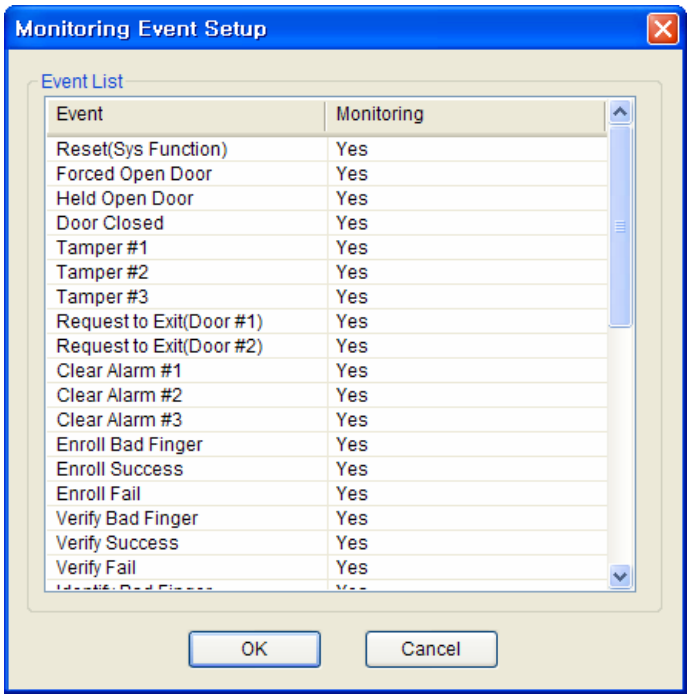
9. Monitoring

BioAdmin supports real time monitoring functions. By selecting the **Monitoring** menu, you can check the log events of networked BioEntry™ readers on time.

** During monitoring mode, most of menus on the command menu bar will be deactivated.



9.1. Setup Monitoring



On this menu, you can select the events to be shown on the monitoring window simply by double clicking on the Yes/No field of each event.

- If you double click the Yes field, it will be changed to No, and the event will not be listed on the monitoring window.
- If you double click the No field, it will be changed to Yes and the event will be listed on the monitoring window.

9.2. Start Monitoring

- By pressing the **Start Monitoring** button, you can start the real time monitoring of the log events from all networked BioEntry™ readers.
- If you select another menu during monitoring mode, monitoring will be stopped.
- Event List on the monitoring window shows up to 5000 events. If the number of events is more than 5000, the oldest event will be automatically deleted from the list. Even though the oldest event is deleted from the monitoring list, it still remains on the log data of BioEntry™ reader.

9.3. Pause Monitoring

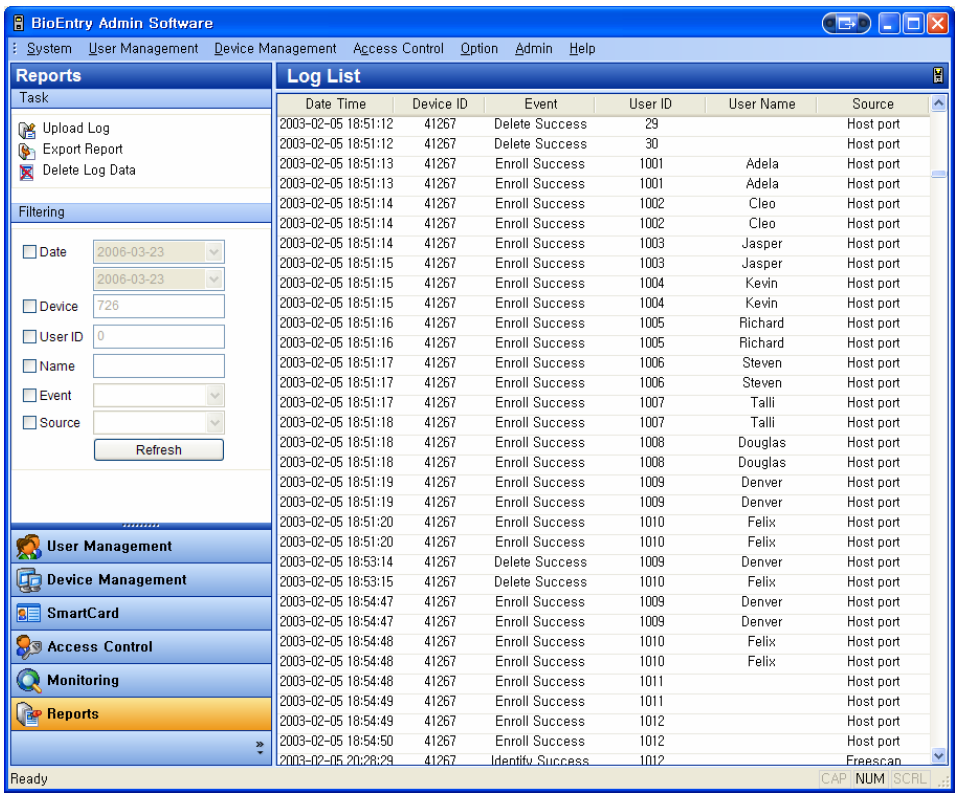
By pressing the **Pause Monitoring** menu, you can stop monitoring.

10. Reports

The Reports menu covers the following operations:

- Management of log database stored on host PC
- Upload new log events from the reader into the log database

By selecting the **Reports** menu, the log list page is updated on the main window.



10.1. Organization of reports page

The Reports page is composed of 2 components:

- Log List

Log database is stored on host PC enabling to preserve old log data. Log list shows stored log events describing Date, Time, Device ID, Event, User ID, User Name, and Source.

- Filtering Tool

You can filter log records by Date, Device, User ID, Name, Event, and Source. For example, if a device is selected, log events of the selected device will be shown.

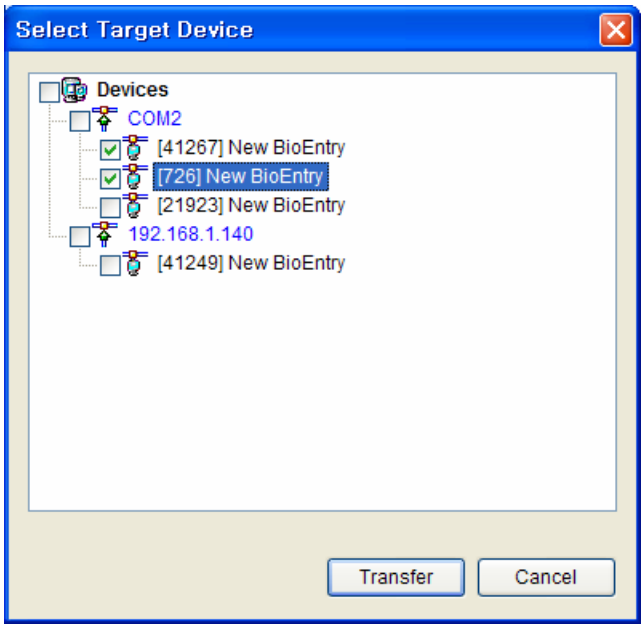
- Task box

Task box includes buttons to control basic operations of the Reports page.

10.2. Log database management

10.2.1. Upload log

In order to upload log data from BioEntry™, press the **Upload Log** button. Then, the new event logs from the selected BioEntry™ will be added to log list.

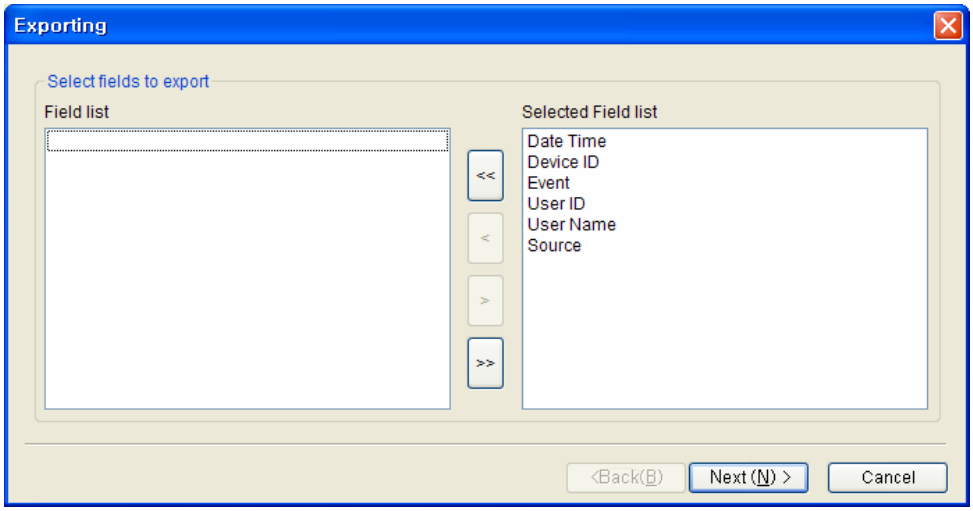


10.2.2. Export Report

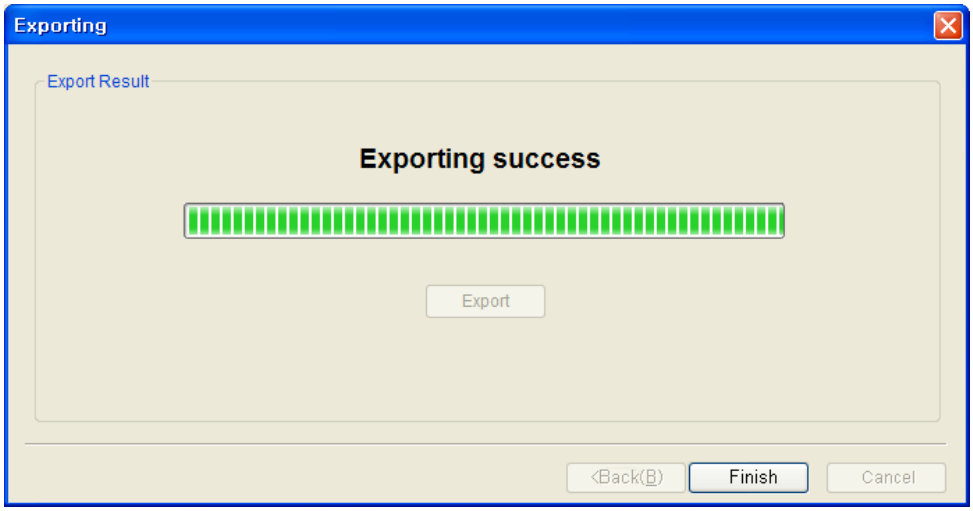
Log data can be exported to CSV file format using the **Export Report** button.

Detailed operations are as follows:

- Press the **Export Report** button.
- Select fields to export by simply moving the target field from Field List to Selected Field List.



- After selecting the fields, press the **Next** button.
- Select a file to export
- After selecting the file, press the **Next** button.
- Press the **Export** button.



10.2.3. Delete Log Data

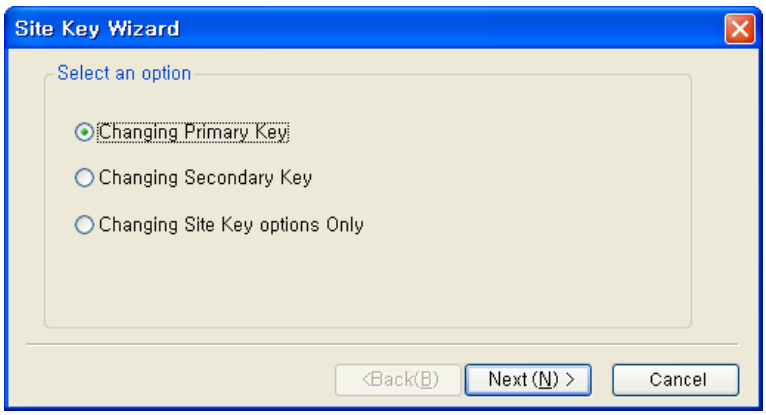
The **Delete Log Data** button eliminates selected log data from log database on host PC. Log data on BioEntry™ are not removed by this command, but automatically removed only when the reader requires space for additional log data.

11. Site Key

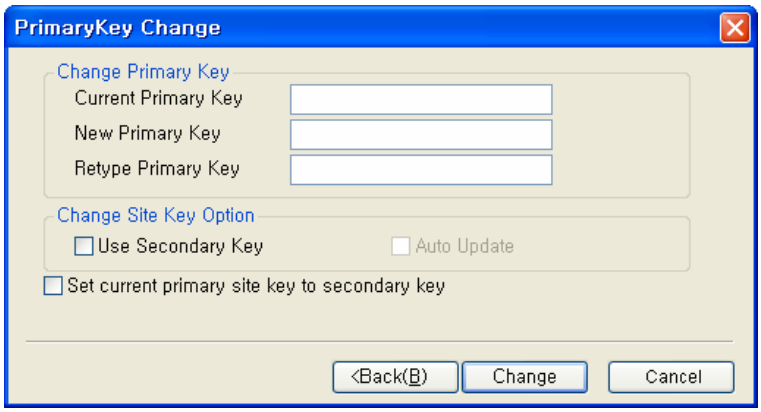
To prevent unauthorized access, Smartcards are encrypted with a 48 bit site key. For a BioEntry reader to decrypt a Smartcard, the site key stored in the reader should match with that of the card. Users can store as many as two site keys in the BioEntry reader and select two advanced options. If the **Use Secondary Key** option is selected, the reader will try both the primary and secondary keys when decrypting a Smartcard. If it is not selected, the reader will try only the primary key. The **Auto Update** option is useful when changing the keys of Smartcards. With this option on, the reader will re-encrypt a Smartcard with the primary key when it is encrypted with the secondary key.

Site keys should be handled with utmost caution. If it is revealed, the whole system is not secure any more. You can change the site keys and options by selecting **Option/Site Key Wizard**.

You can find the **Site Key Setting** menu below the **Device Management** menu on **Common menu bar**.



11.1. Primary Key

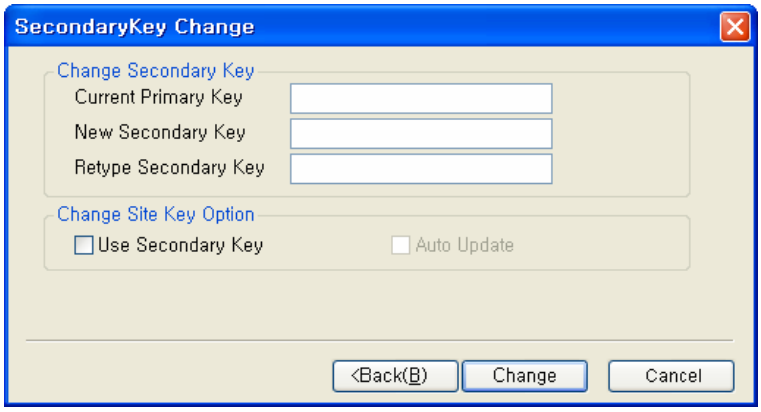


To change the primary key, you should enter the current and new primary keys. Besides the **Auto Update** option, you can also select the following options.

- **Set current primary site key to secondary key**: Replaces the secondary key with the current primary key before changing the primary key.

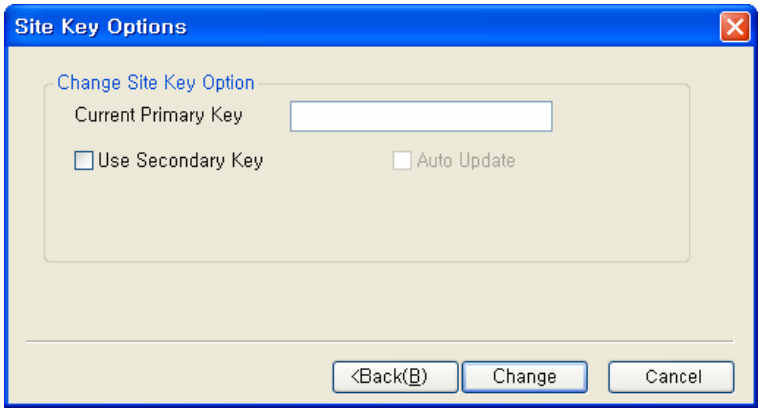
11.2. Secondary Key

To change the secondary key, you should enter the current primary key and the new secondary key.



11.3. Key Options

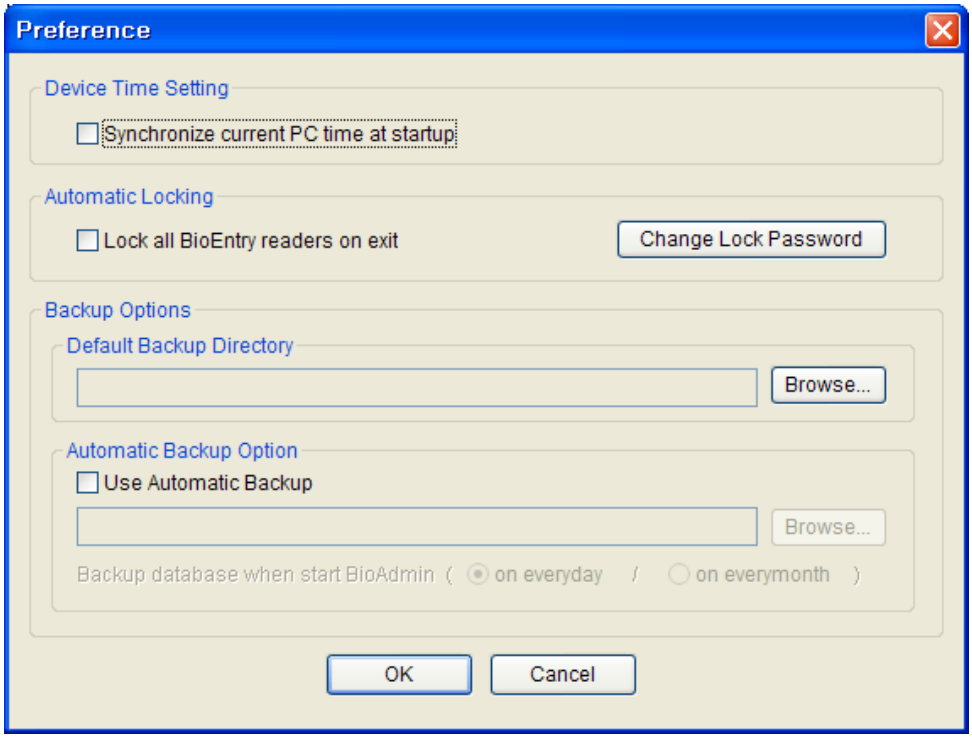
You can also change the key options only. In this case, you only have to enter the current primary key with the options.



12. Preference

On the preference menu, the following functions are supported.

- Device Time Setting
- Automatic locking and password management of BioEntry™
- Backup user database and log database on host PC

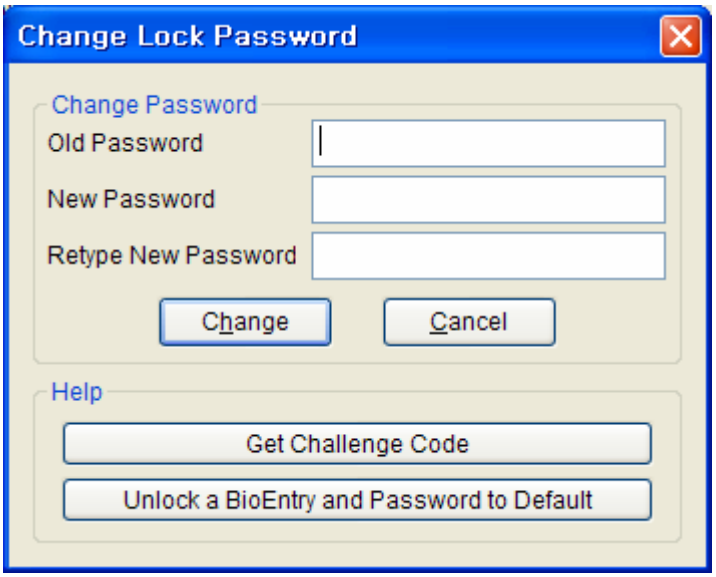


12.1. Device Time Setting

By checking on the **Synchronize current PC time at startup** check box on the Preference window, you can synchronize the time of all networked BioEntry™ to the time of host PC.

12.2. Automatic Locking and Password Management

BioEntry™ readers can be locked by password to enhance the security. If the locked BioEntry™ is found on the network, BioAdmin software requests to enter password to unlock BioEntry™. Locking mechanism is enabled by the **Lock all BioEntry readers on exit** check box in this window or the **Lock All Readers** menu below the **System** menu in **Command menu bar**. If it is enabled, BioAdmin software locks the readers at termination of the program. The **Change Lock Password** button initiates the password management window.



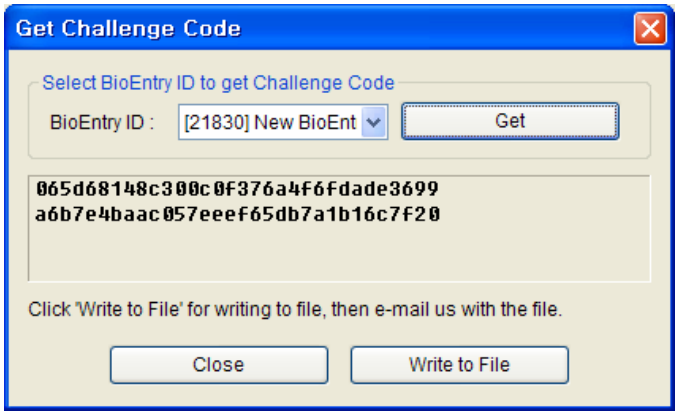
12.2.1. Changing locking password of BioEntry™ readers

Locking password of BioEntry™ readers are changed by typing old and new password and pressing the **Change** button. Locking password is not stored by BioAdmin software. **Administrator should remember the password when using this locking mechanism**.

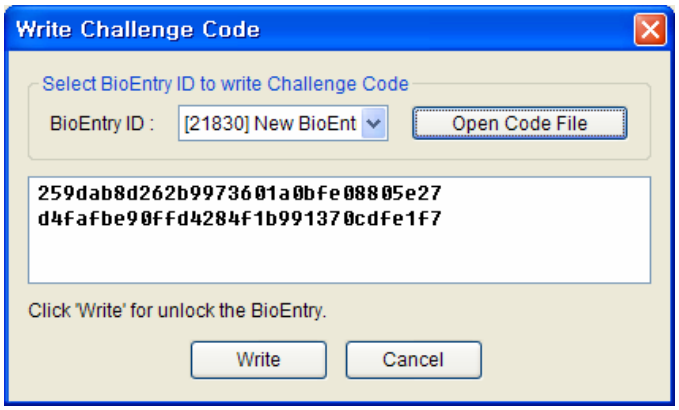
12.2.2. Resolving the locked readers

If the readers are locked but cannot be unlocked in case of forgetting password, the following procedures are required.

- Obtain a challenge code file using the **Get Challenge Code** button and send the file to technical support team (support@supremainc.com)



- The support team will send you the unlock code file corresponding to the challenge code. Use **Unlock a BioEntry and Password** to the **Default** button to resolve the reader. Then, the reader is unlocked and password is changed to default (null).



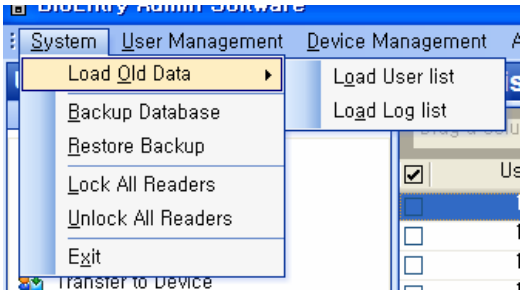
12.3. Backup Options

- Default backup directory: Default backup directory for database can be specified on the preference page. Related backup files will be stored on the specified directories.
- Automatic Backup Option: By checking on the **Use Automatic Backup** check box, you can automatically save the backup database whenever you close the BioAdmin software.
- You can select the period of the automatic backup between everyday and every month. This automatic backup replaces the old database with the new database at the termination of BioAdmin software.

13. Miscellaneous functions

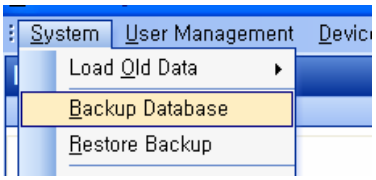
Command menu bar has several miscellaneous functions.

13.1. Load Old Data

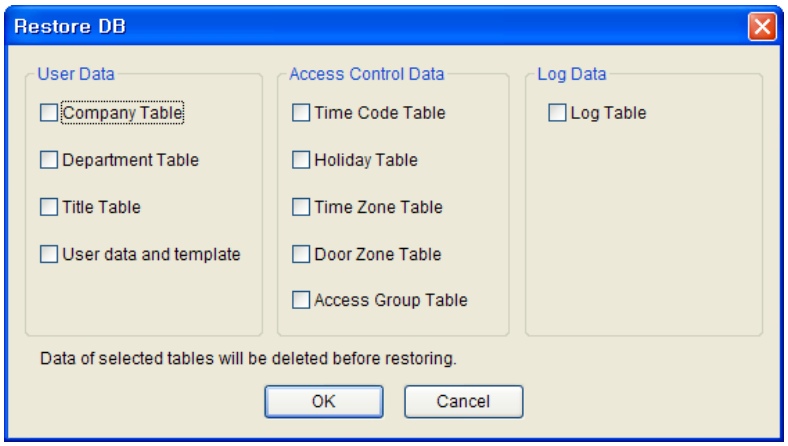


- By clicking the **Load Old Data** menu, you can import old user data and log data which was made before installing BioAdmin Software version 2.0. By executing this menu, the existing database is deleted and replaced with the loaded old data. Therefore, this menu is to be used only for the initial execution of BioAdmin software version 2.0.

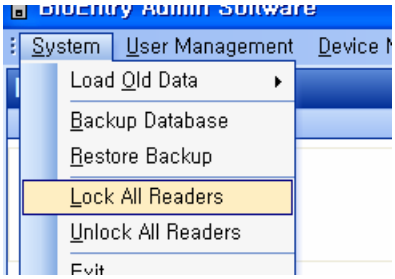
13.2. Backup Database / Restore Backup



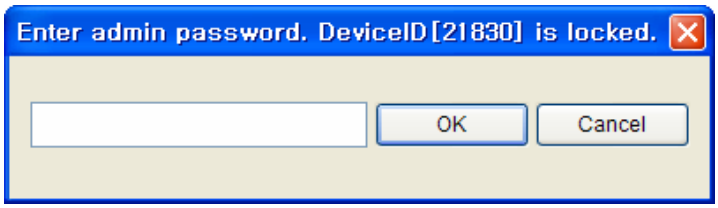
- Aside from the Automatic Backup on Option menu, you can make a back up file manually and restore the database from this back up file.



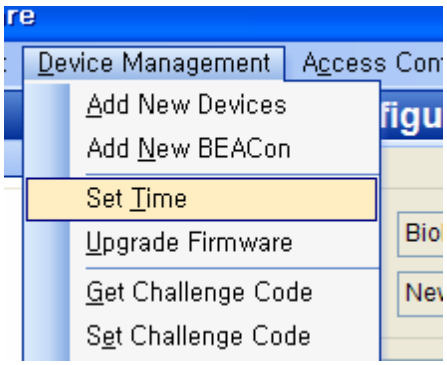
13.3. Lock All Readers / Unlock All Readers



- You can lock / unlock BioEntry™ reader while you are using BioAdmin Software. If you click the Lock All Readers menu, all of networked BioEntry™ readers will be locked. Once the BioEntry is locked. It will not respond to any external packet, only except the unlock command. On the other hand, you can unlock all of the locked BioEntry™ readers by clicking the on the Unlock All Readers menu. If a locking password was set up, you need to enter the password to lock/unlock BioEntry™.

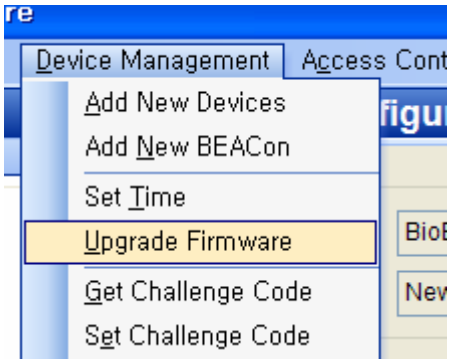


13.4. Set Time

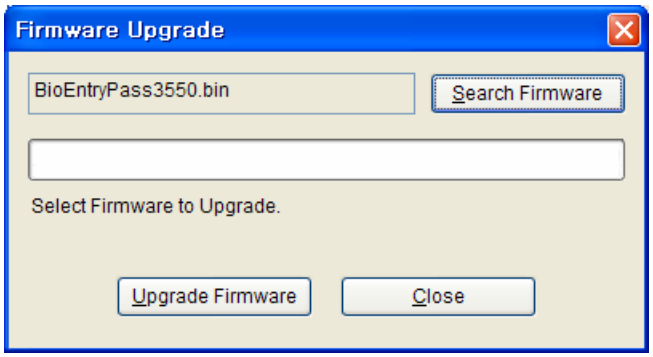


- You can synchronize the time of all of the networked BioEntry™ to the time of host PC. If you already checked on the **Synchronize current PC time at startup** check box, which is on Options → Preference → Device Time Setting, you do not need to synchronize the time on this menu.

13.5. Upgrade Firmware



- By selecting the Firmware Upgrade menu, a pop-up window for firmware upgrade appears:



- 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 might be impossible.
- Firmware upgrade is processed for one reader. Selection of a group or all readers is not allowed.

Contact Information

Suprema Inc.

16F Parkview Office Tower, Jeongja-dong, Bundang-gu,

Seongnam, Gyeonggi, 463-863 Korea

Tel: +82-31-783-4502

Fax: +82-31-783-4503

Web site: http://www.supremainc.com

Sales inquiries: sales@supremainc.com

Technical inquiries: support@supremainc.com