BioAdmin Manual

Version 4.1

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 BioEntry and BioStation

BioEntry and BioStation are biometric access control and time attendance device with algorithms awarded grand prix at finger scan contest (FVC2004) and standard Wiegand interface. BioEntry and BioStation can replace an existing system or be added to an existing access control and time attendance system with ease.

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

BioEntry Pass is a fingerprint access device 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.

BioStation is the access control and time attendance finger terminal of distinguished performance. Multifunctional fingerprint terminal for access control and time and attendance, BioStation provides various information real time adopting 2.5 inch color LCD and high-quality sound. Also, using wireless LAN or USB memory, you can configure network and transfer data without complicated wiring.

BioEntry and BioStation supports various fingerprint sensors, i.e. Optical, semiconductor type (capacitive type) or scan type (swipe thermal type),

enabling a user to utilize an optimum fingerprint sensor fit for the application system.

About Suprema Inc

Suprema is a leading biometric company offering core fingerprint technologies in various applications. Suprema's fingerprint products include access control systems, time attendance system, low cost standalone OEM modules, 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 80 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 and BioStation. This manual describes how to manage templates, properly adjust relevant parameters, enroll or delete templates, etc. The purpose of this manual is to provide instructions to using BioEntry and BioStation and troubleshooting tips.

Table of contents

Revision History

Version	Date	Description
V1.0	2005.9.27	Created.
V1.1	2005.12.2	Incorporated the changes made by BioAdmin V1.1. Chapter 12. Site Key is added.
V2.0	2006.4.17	Incorporated the changes made by BioAdmin V2.0. Chapter 8. Access Control is added. Chapter 9. Monitoring is added.
V3.0	2006.8.23	Time Attendance added BioStation added.
V4.0	2007. 3. 5	Incorporated the changes made by BioAdmin V4.0.
V4.1	2007. 5. 30	Incorporated the changes made by BioAdmin V4.1.

1. Getting Started

1.1. Outline

This manual illustrates how to use BioAdmin software. BioAdmin is a PC Windows software for the control and management of Suprema's BioEntry, BioStation and BEACon products. BioAdmin includes various functions needed for a host station for applications of access control and time & attendance using these devices.

For proper hardware connection, please refer to BioEntry Installation manual and BioStation Installation manual.

There are two approaches in managing BioEntry and BioStation. :

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

1.2. Fundamentals

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

1.2.1. Finger scan device

Fingerprint access device 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 device can be substituted for existing access devices, such as barcode, magnetic card, keypad, or RF card devices, with high security and efficiency.

1.2.2. Finger scan smart card device

Fingerprint smart card device is an advanced model of fingerprint access device

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 device authenticates the user by comparing the stored fingerprint data in the smart card with the input fingerprint data.

1.2.3. 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 device or on user's smart card. In authenticating a user, a new template is also generated and compared with the stored templates.

1.2.4. Enrollment

Enrollment is the process to store the fingerprint template with user information. Through enrollment process, new users are entered into the system.

1.2.5. 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 device carries out verification process by scanning an input fingerprint. On BioEntry Pass, verification process can be implemented by connecting external Wiegand device, such as RF card device, which provides the current user ID.

1.2.6. Identification

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

1.2.7. User database

User database includes user ID, user name, fingerprint templates, and so on. BioAdmin 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 and BioStation connected on the network using transfer menu.

1.2.8. Transfer

Transfer to Device is used to transfer the user database of the host PC to BioEntry and BioStation. 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 and BioStation
- Replace inconsistent templates on BioEntry and BioStation
- Delete templates of unknown users or de-selected users on BioEntry and BioStation

Transfer from Device is used to upload the user formation from BioEntry and BioStation 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.

1.2.9. 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.

1.3. How to place a finger

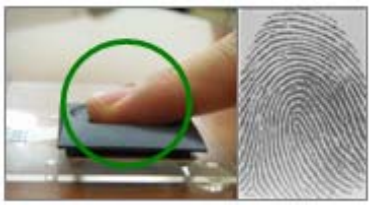
1.3.1. Select a finger to enroll

(1) It is recommended to use an index finger or a middle finger.
(2) Thumb, ring or little finger is relatively more difficult to place in a correct position.

1.3.2. How to place a finger on a sensor

(1) Place a finger as it completely covers the sensor with maximum contact.
(2) It is better to place the core part of a fingerprint to the center of a sensor.
    - People usually tend to place only the top end of a finger
    - Where is the core (center) of a fingerprint?
        - A peak where spirals of fingerprint ridges are dense
        - Usually opposite to lower part of a nail
        - It is recommended to place a finger as the lower part of a nail is located at the center of a sensor

(3) If a finger is placed as in the right picture, only a small area of a finger is captured. So it is recommended to place a finger as in the left picture.



1.3.3. Tips for different finger conditions

Suprema's fingerprint products are designed to scan fingerprint smoothly regardless of the conditions of a finger skin. However, if a fingerprint is difficult to scan due to other influences, please refer to the followings tips.

(1) If a finger is stained with sweat or water, scan after wiping moisture off
(2) If a finger is covered with dust or impurities, scan after wiping them off
(3) If a finger is way too dry, scan after blowing warm breath on a fingertip.

1.3.4. Advices on fingerprint enrollment

(1) In fingerprint recognition, enrollment process is very important. Therefore, when enrolling a fingerprint, please try to place a finger correctly with care.
(2) In case of low acceptance ratio, the following actions are recommended.
   - Delete enrolled fingerprints and re-enroll the fingers.
   - Enroll the same finger additionally
   - Try with another finger if a finger is not easy to enroll due to scar or worn-out.
(3) For the case when an enrolled fingerprint can't be used due to scar or holding a baggage, it is recommended to enroll more than two fingers.

1.4. Concept of BioAdmin 4.1

BioAdmin 4.1 is operated as server-client application so that users can operate the BioAdmin Client program from multiple host PCs at the same time. If the users connect BioStation to the BioAdmin Server, logs from the BioStation will be automatically stored on the database of BioAdmin Server real-time. In this server-client application, BioAdmin Client is used as the user interface to manage the data.

If the user does not connect the BioStation to the BioAdmin Server, logs will not be

stored on the database automatically.

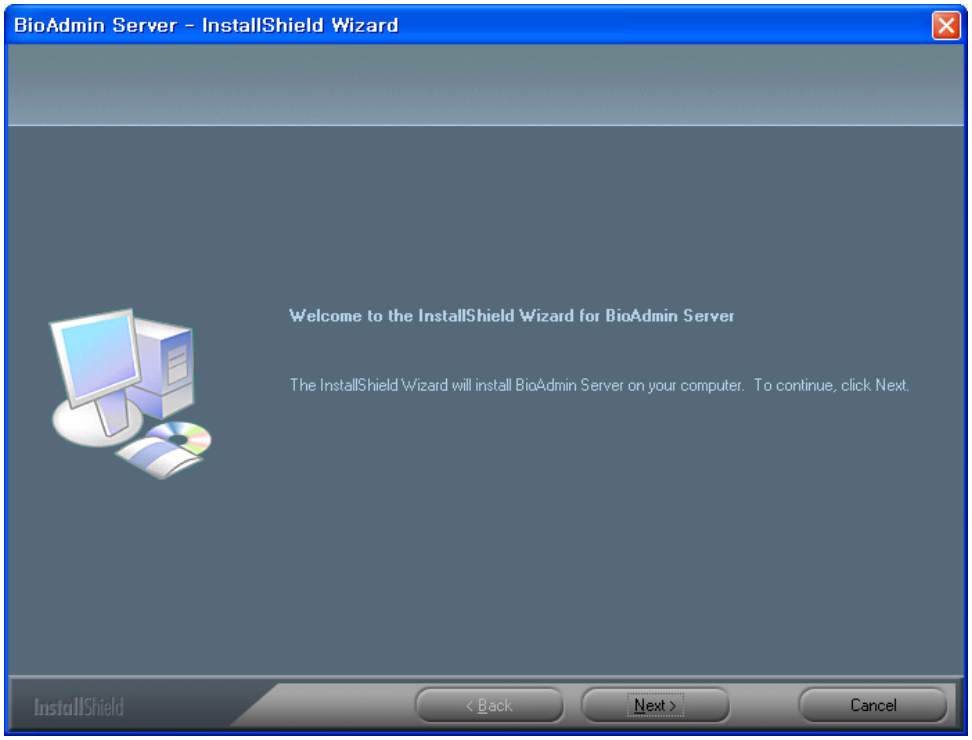
BioAdmin Server is designed only for BioStation. Therefore, you can not use the BioEntry or BEACon as the server-client application.

This chapter describes the installation and operation of BioAdmin Server and BioAdmin Client programs.

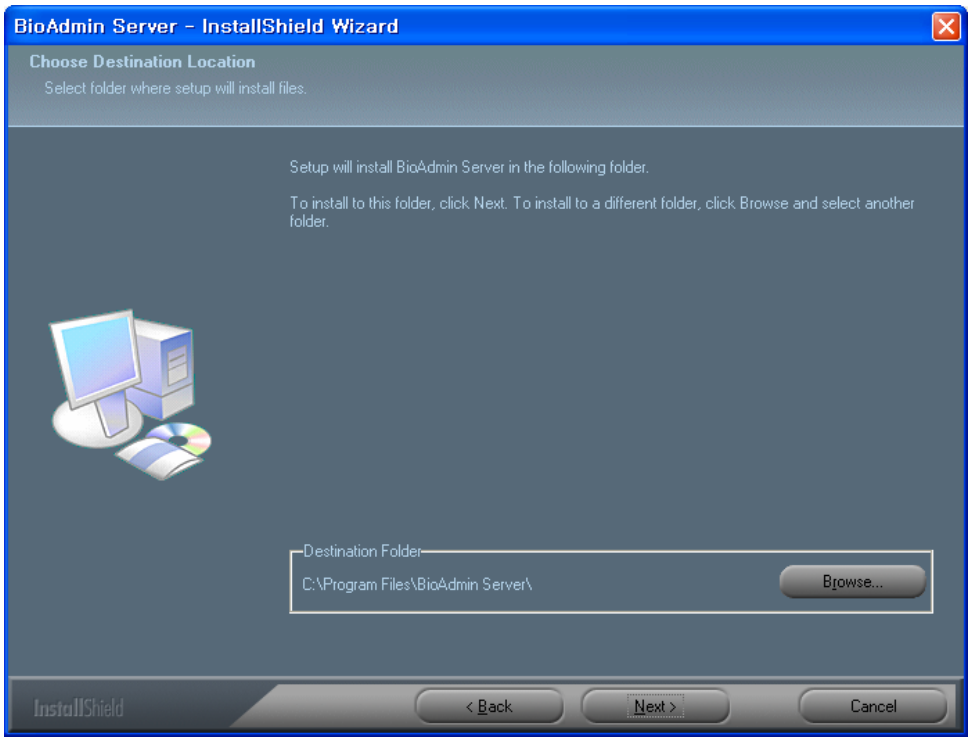
1.4.1. How to install BioAdmin Server

- Select the PC to be used as the server. Server PC should be always tuned on , because it should receive log data from the connected BioStation and store it on the database real time.
- After selecting a PC to use as the BioAdmin Server, install the BioAdmin Server program. This chapter shows the installation process under the condition that you are using the database on your host PC. If you are using MySQL or SQL Server, you can refer to the chapter 1. 4. 3.

- Start Installation.



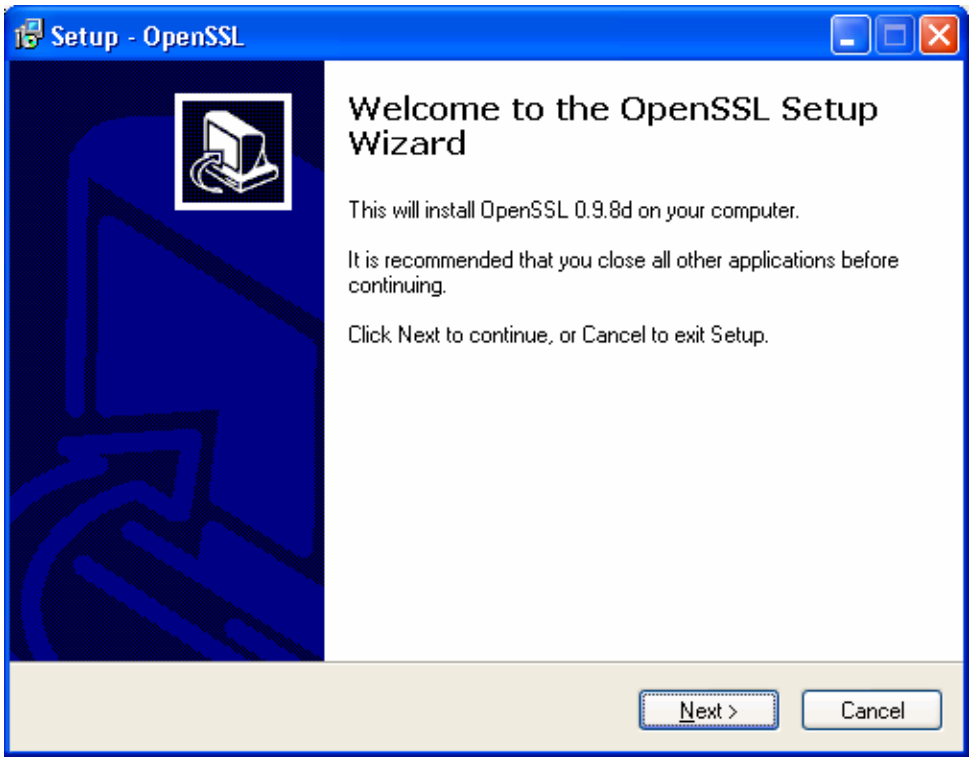
- Choose Destination Location



Choose the hard disk drive on which BioAdmin Server is to be installed. By

default, BioAdmin Server is installed in C:\Program Files\BioAdmin Server\.

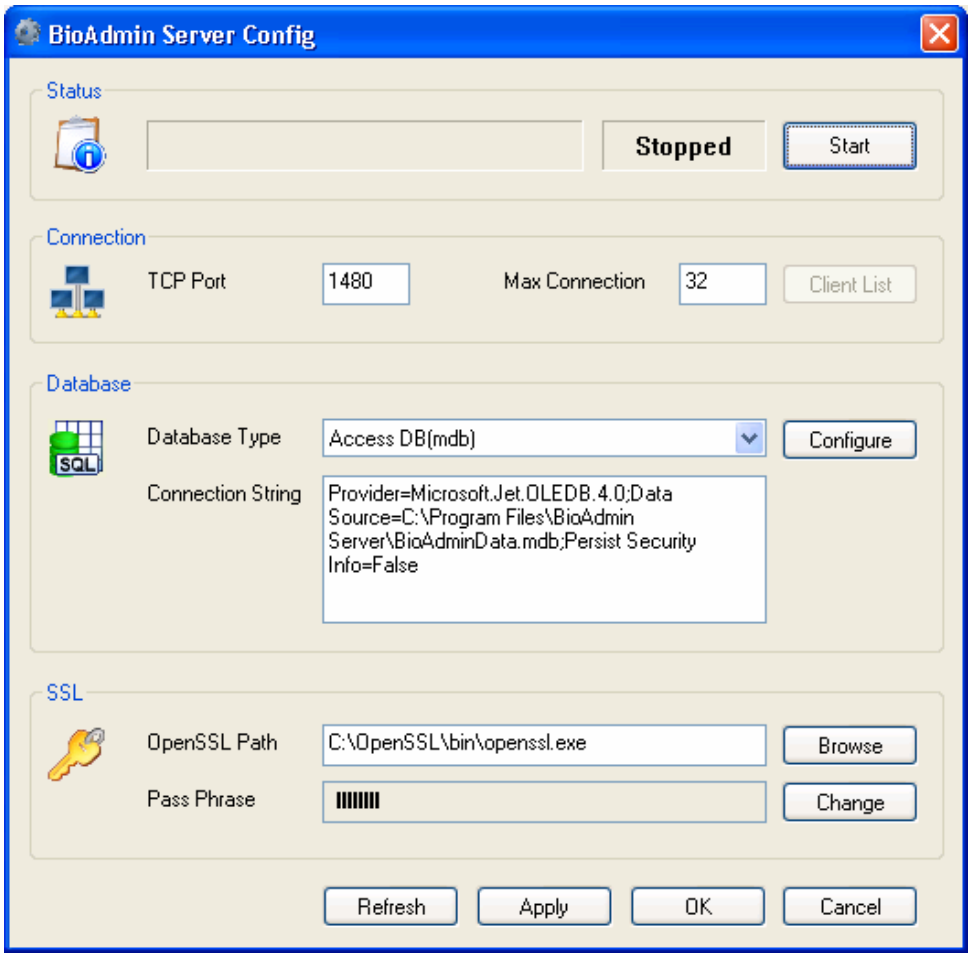
- Setup Open SSL



After copying all files, set up the Open SSL.

- BioAdmin Server Configuration and Database Setting

  If you finish the Open SSL set up, following window will appear which is to set up the BioAdmin Server configuration. In most cases, you can maintain its default value for the BioAdmin Server configuration.



- Status

Status shows the current version and status of the BioAdmin Server. By pressing **Start** or **Stop** button, you can start or stop the operation of BioAdmin Server.

If BioAdmin Server is stopped, logs from the networked BioStation will not be stored on the database of the BioAdmin Server and BioAdmin Client will not be able to access to the BioAdmin Server.

If you changed any server configuration or database setting, stop the BioAdmin Server and restart it. Before you restart the BioAdmin Server, changes in the BioAdmin Server configuration or database will not be applied to the BioAdmin Server.

- Connection

On this menu, you can set up the networking details.

- TCP Port

Enter the TCP port. This TCP port is used when you attach a BioStation to the BioAdmin Server or when you access to the BioAdmin Server from BioAdmin Client. Use a unique port, which is not used by any other software.
In most cases, you can use the default port, 1480.

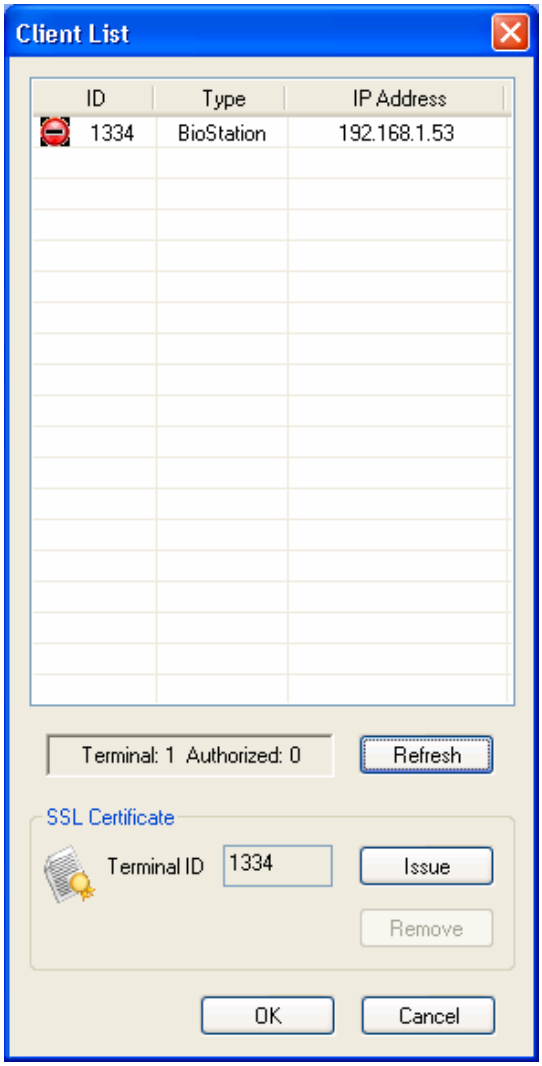
- Max Connection

Enter the maximum number of BioStation or BioAdmin Client, which can be connected to the BioAdmin Server at the same time. For example, if you designate it as 50, the total number of BioStation and BioAdmin Client, which can be connected to the BioAdmin Server simultaneously, will be 50.

Maximum number for this connection should be less than 128. If the number is less than 32, which is the default value, you do not need to lower this number from the default.

- Client List

Client List shows the list of BioStations, which are connected to the BioAdmin Server. This list shows the IP Address of those connected BioStations and indicates whether the SSL Certificate was issued. You can issue or remove the SSL Certificate on this list. If the BioAdmin Server is stopped, this menu will be deactivated.



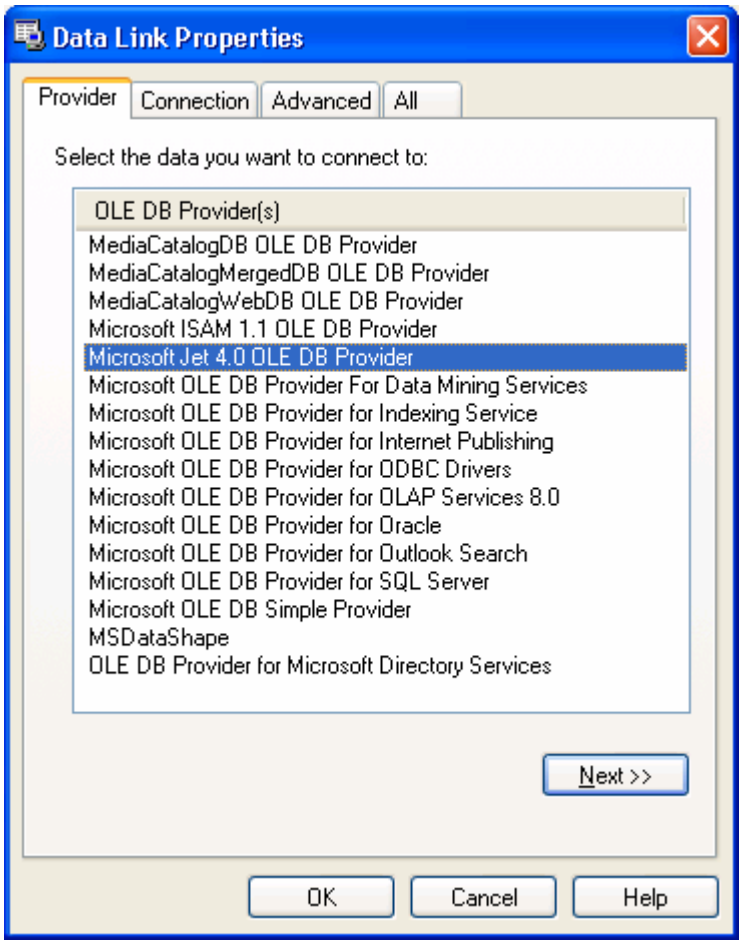
- Database

Select the database type of the BioAdmin Server. BioAdmin Server uses Microsoft Access Database by default. If you are not using any external database, leave this field just as its default, MS Access DB (mdb).

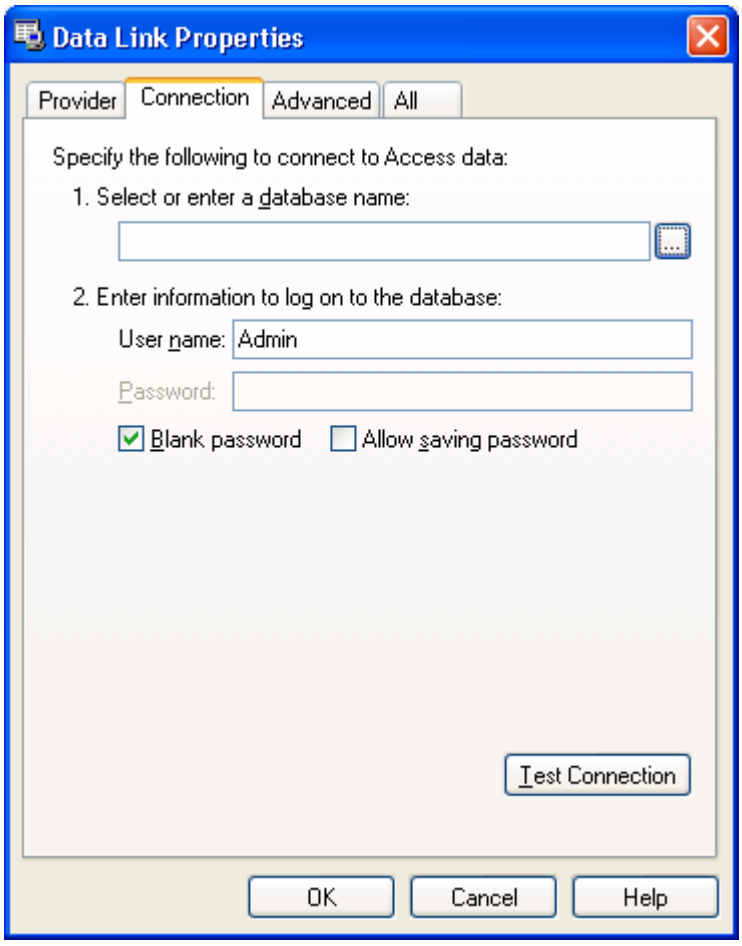
Additionally, if you are already using MySQL or SQL Server, BioAdmin Server also supports MySQL and SQL Server. However, BioAdmin Server does not provide any new installation of the MySQL or SQL Server.

For the details of the database management, refer to the chapter 1. 4. 3.

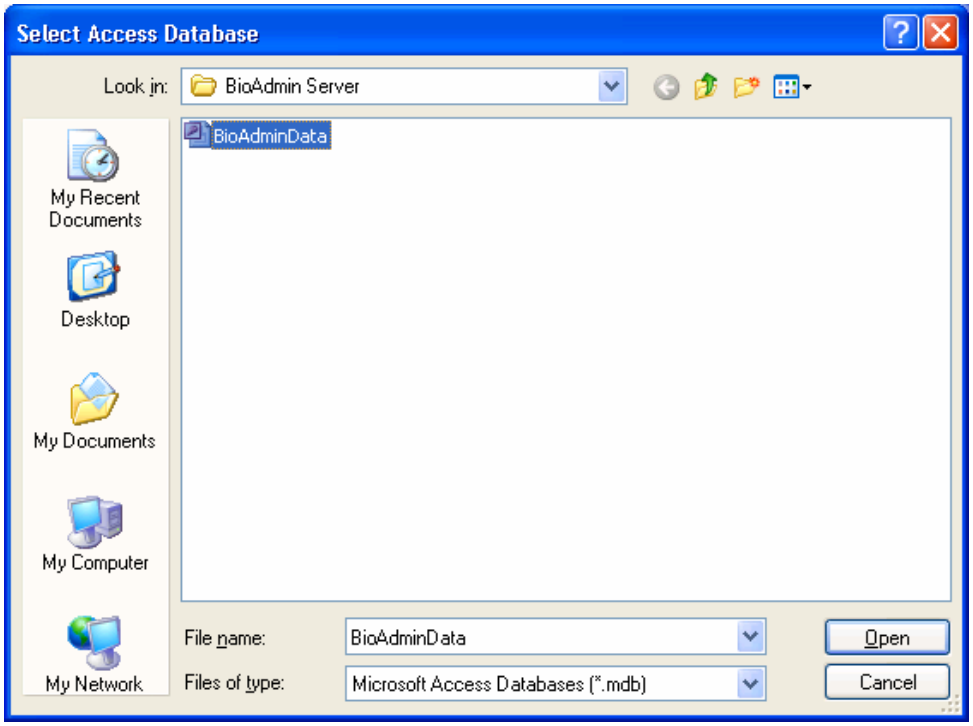
After selecting the database type, press **Configure** button and set up the database. If you are using the default mdb file, select Microsoft Jet 4.0 OLE DB Provider.



Press **Next** button.



Select the Database file and press **OK** button.



- SSL

Set up the encryption details between BioAdmin Server and BioAdmin Client or between BioAdmin Server and BioStation.

Press **Refresh** button to show the current setting.

Press **Apply** button to store the new setting. To apply the changes, you should stop and restart the BioAdmin Server.

Press **OK** button to store the new setting and close the BioAdmin Server Config window.

Press **Cancel** button to cancel the new setting and close the BioAdmin Server Config window.

- OpenSSL Setting

BioAdmin Server uses a encrypted communication with BioAdmin Client and BioStation by using SSL authentication. Encrypting the communication between

BioAdmin Server and BioAdmin Client (or BioStation) enables much more secure solution to protect the information.

Designate the OpenSSL path. By default, you can find the file on the following directory. If it is installed in any other directory, click the “Browse” and designate the correct directory.

Default directory of the openssl.exe : (C:\OpenSSL\bin\openssl.exe)

Pass Phrase is required to issue the certificate. You should enter more than 8 digits, combination of English, number, or special character. To make the system secure, you are strongly recommended to change the Pass Phrase upon the initial installation of BioAdmin Server.

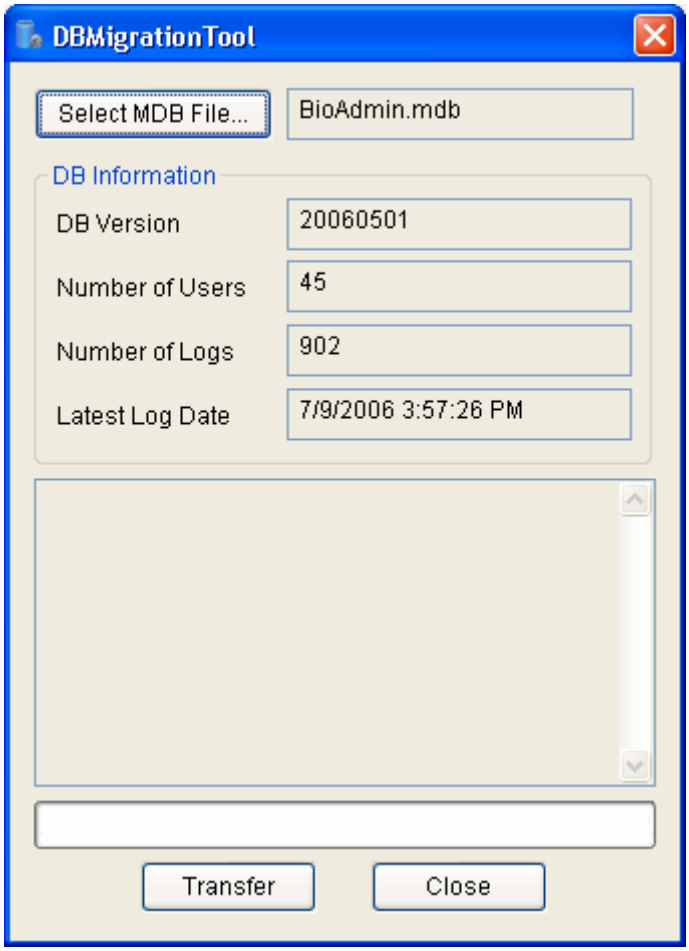
If you change this Pass Phrase while using the BioAdmin Server after the installation, you should conduct the following procedures.

- Change the SSL option of the connected BioStations as Not Use.
- Stop the BioAdmin Server.
- Change the Pass Phrase.
- Start the BioAdmin Server.
- Issue the SSL certificate for BioStation.
  If you are using BioAdmin Client, select the BioStation and press the right button of the mouse. Select **Authenticate Device**.
- If the certificate is issued properly and stored on the BioStation, BioStation will restart automatically.

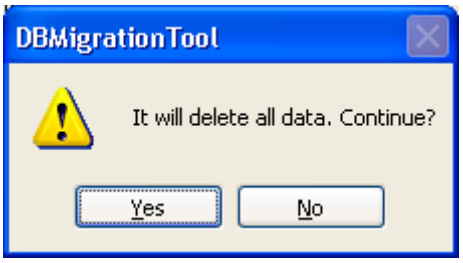
- DB Migration Tool

If you were BioAdmin version 3.X, you need to convert the data from BioAdmin 3.1 to BioAdmin 4.X.

If you do not need the old data, press **Close** button.

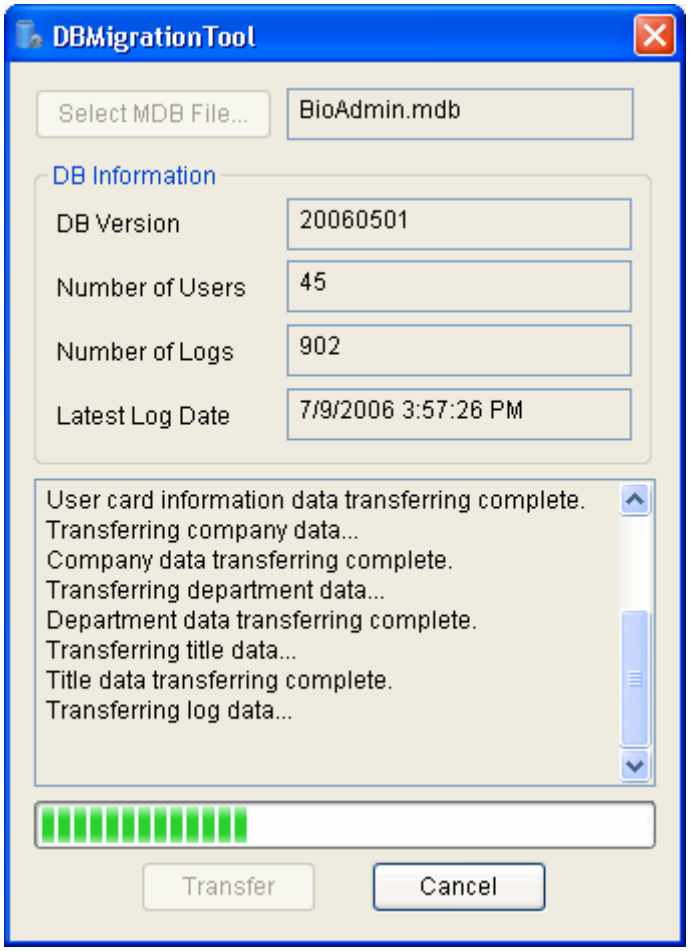


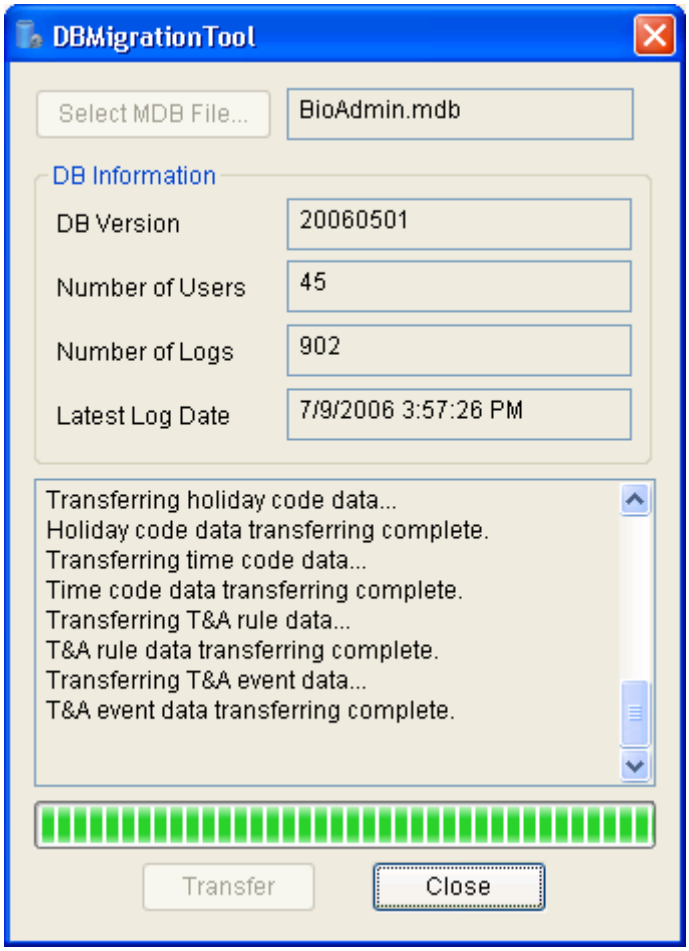
Select the old BioAdmin.mdb file.



Press **Transfer** button to transfer the old data to BioAdmin 4.X.

If you transfer the old data, old data will be deleted. Therefore, if necessary, back up the old data before transferring to BioAdmin 4.X. This data transfer may take time depending on the size of the existing database.


DBMigrationTool
Select MDB File...
BioAdmin.mdb
DB Information
DB Version
20060501
Number of Users
45
Number of Logs
902
Latest Log Date
7/9/2006 3:57:26 PM
User card information data transferring complete.
Transferring company data...
Company data transferring complete.
Transferring department data...
Department data transferring complete.
Transferring title data...
Title data transferring complete.
Transferring log data...
Transfer
Cancel



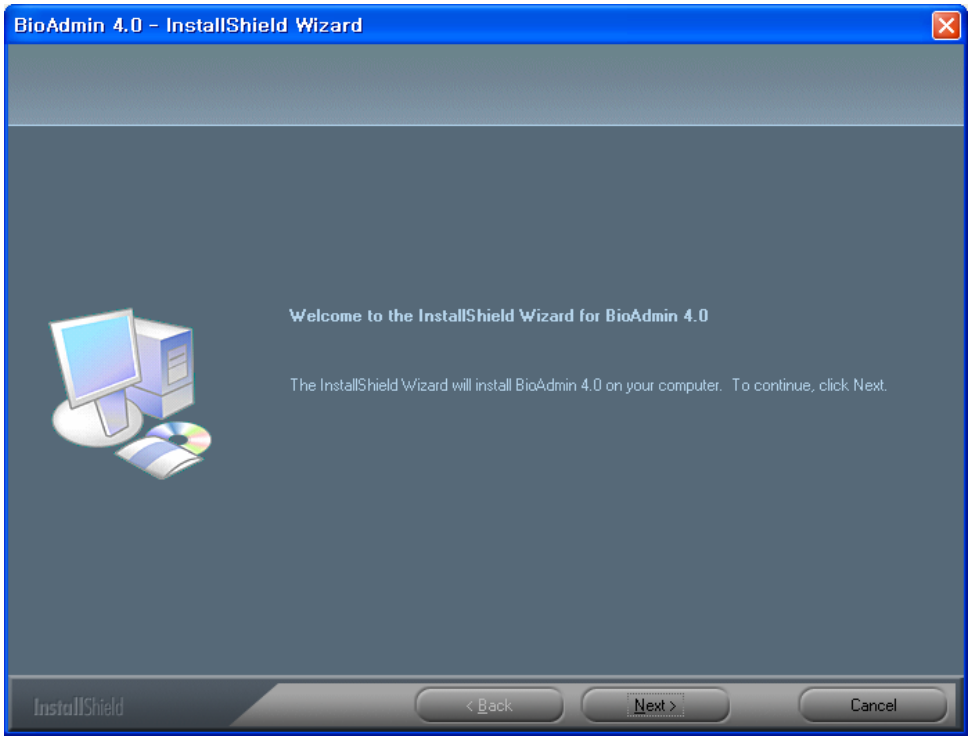
After the transfer, press **Close** button.

- Installation Complete

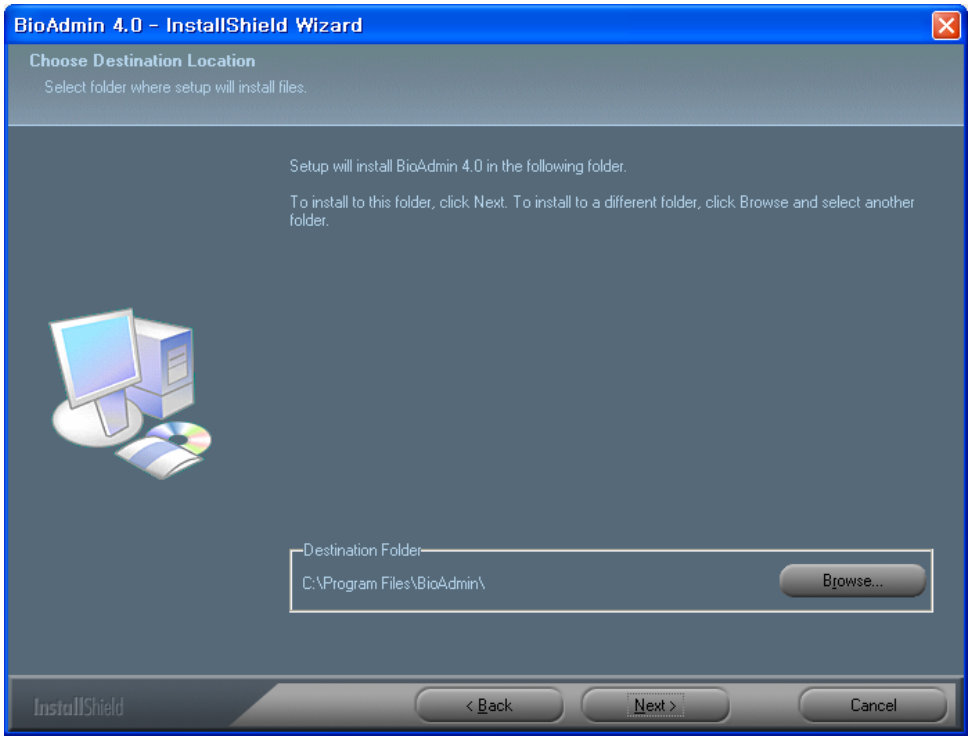
BioAdmin Server was successfully installed. If you are using the OS Windows 2000 or XP, BioAdmin Server will start as its background service. After this initial installation, BioAdmin Server will run automatically.

1.4.2. How to install BioAdmin Client

- Start Installation.

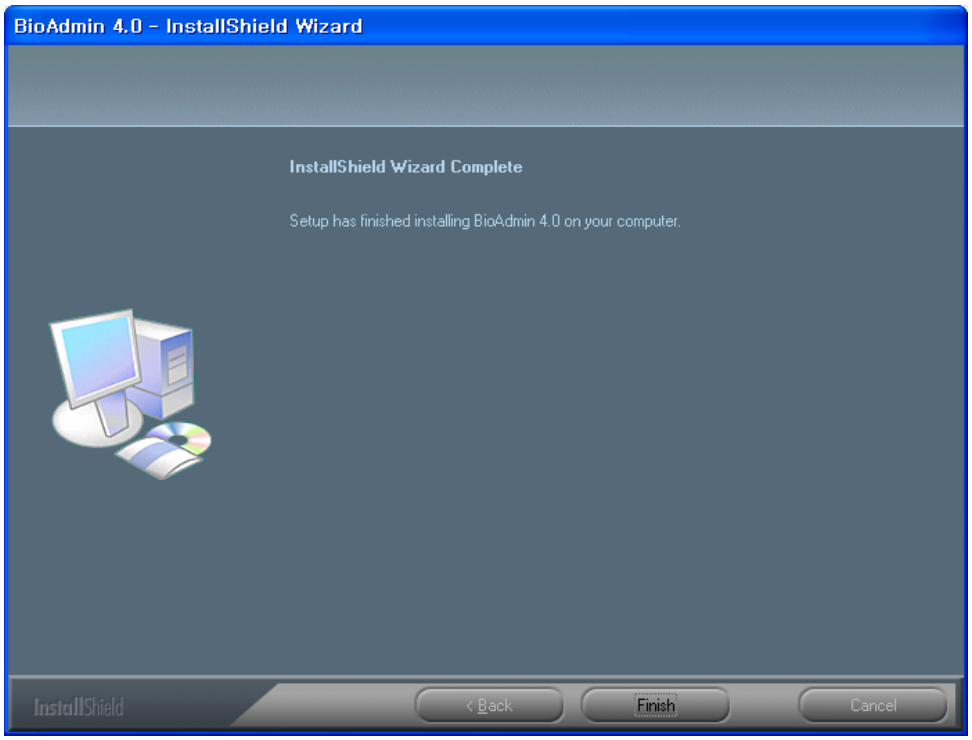


- Choose Destination Location



Choose the hard disk drive on which BioAdmin Client is to be installed. By default, BioAdmin Client is installed in C:\Program Files\BioAdmin.

- Installation Complete



BioAdmin Client was successfully installed. Close the installation program and execute the BioAdmin Client.

1.4.3. Using MySQL or SQL Server database

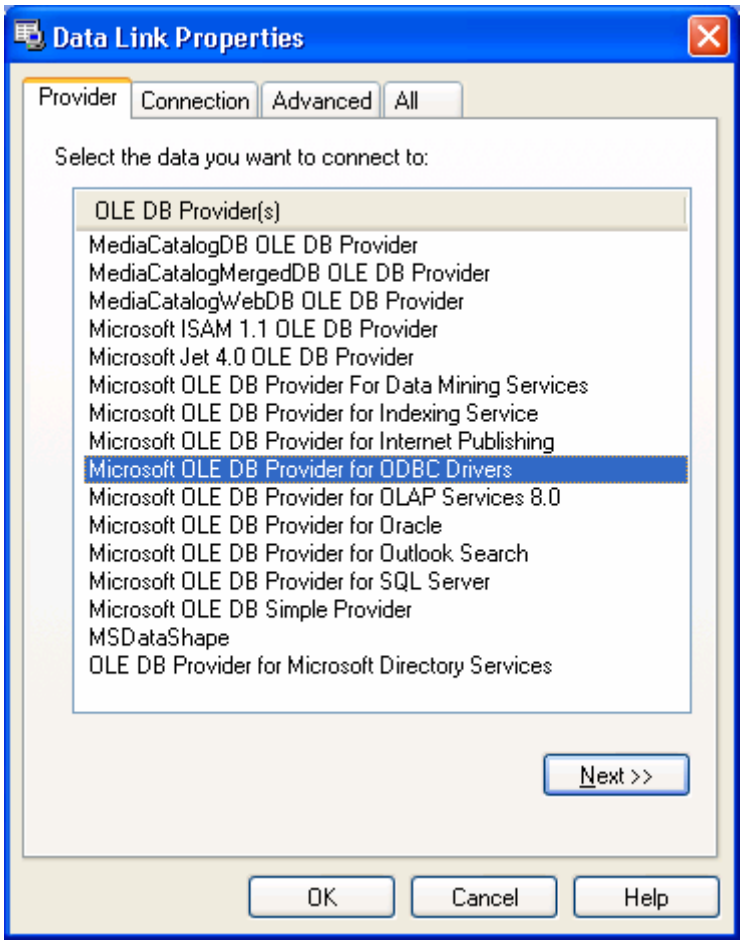
You can use MySql or SQL Server database by the following procedures.

- Using MySQL database

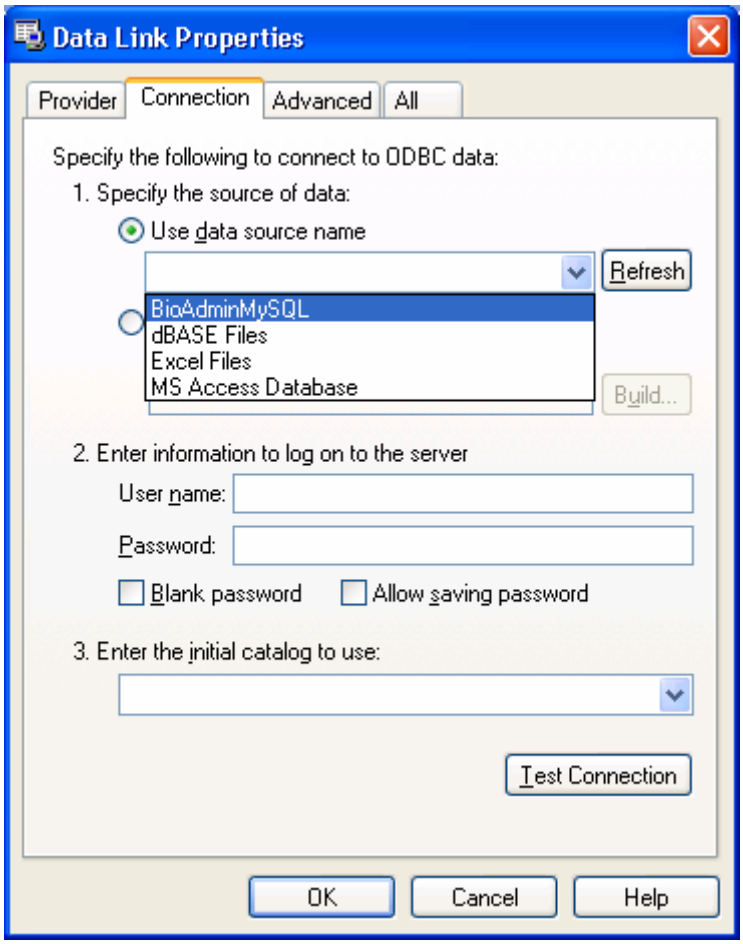
If you are already using MySQL Server, you can use the MySQL database instead of mdb.

- Execute **BioAdmin Server Config** menu.
- Click the **Configure** button on the Database field.

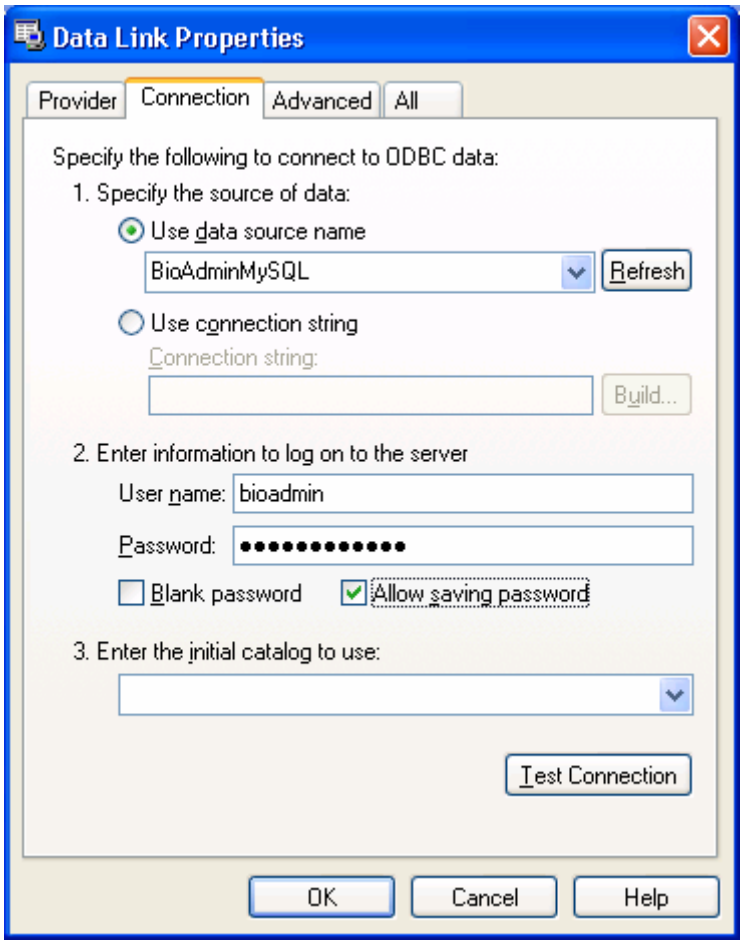
- On the **Data Link Properties** window, select **Microsoft OLE DB Provider for ODBC Drivers** and press **Next** button.



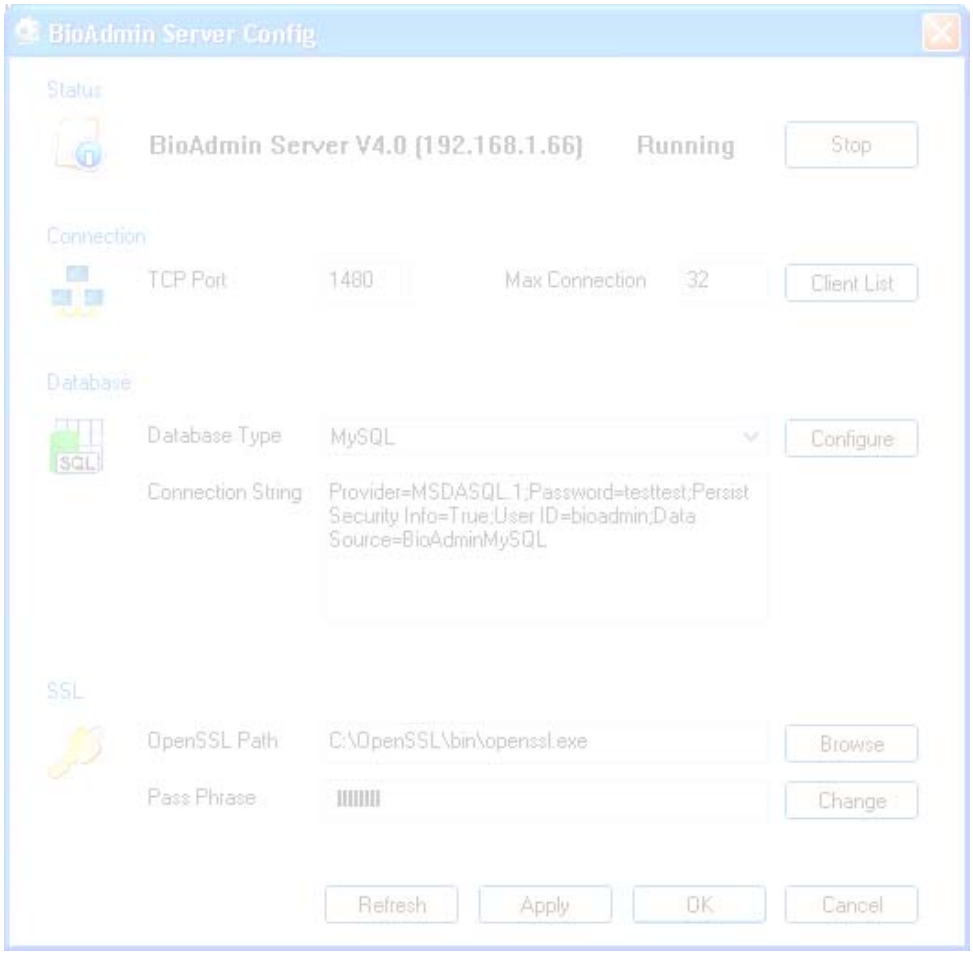
- Select data source name.



- Enter the ID and password of the DB server. It there is no password designated, check on the **Blank password**. If there is any password, check on the **Allow saving password**.

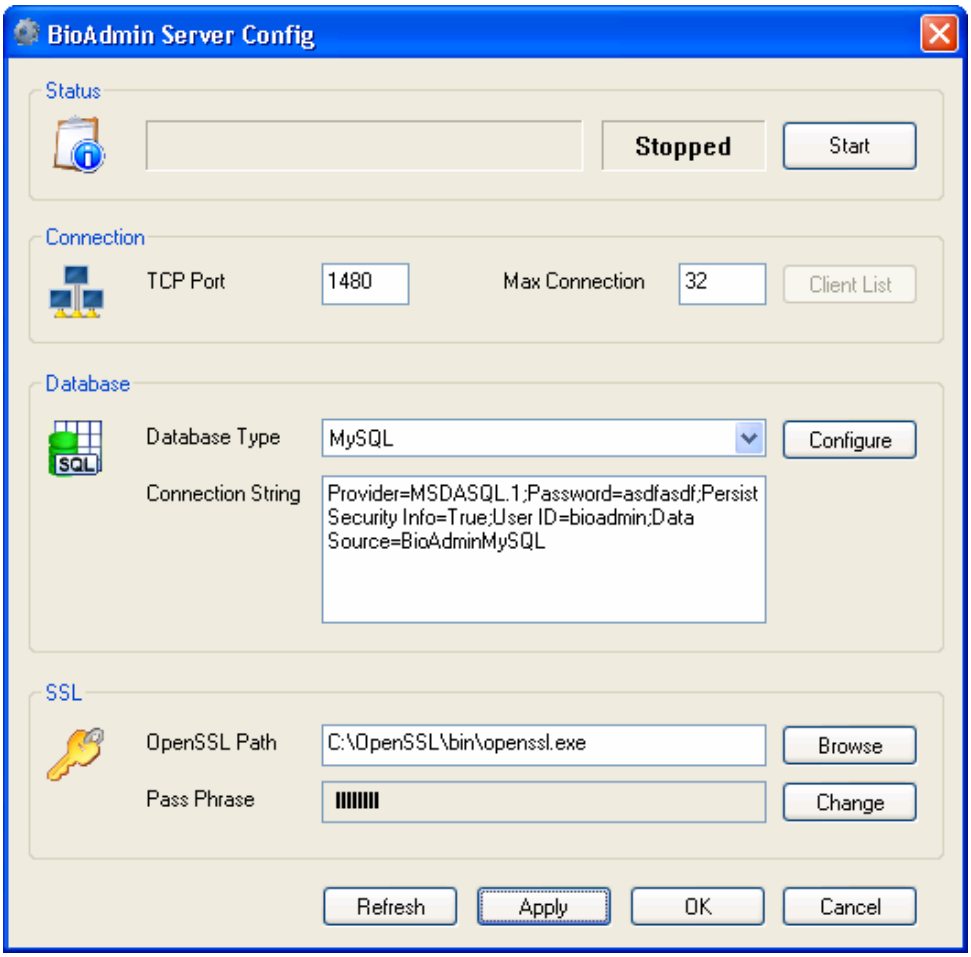


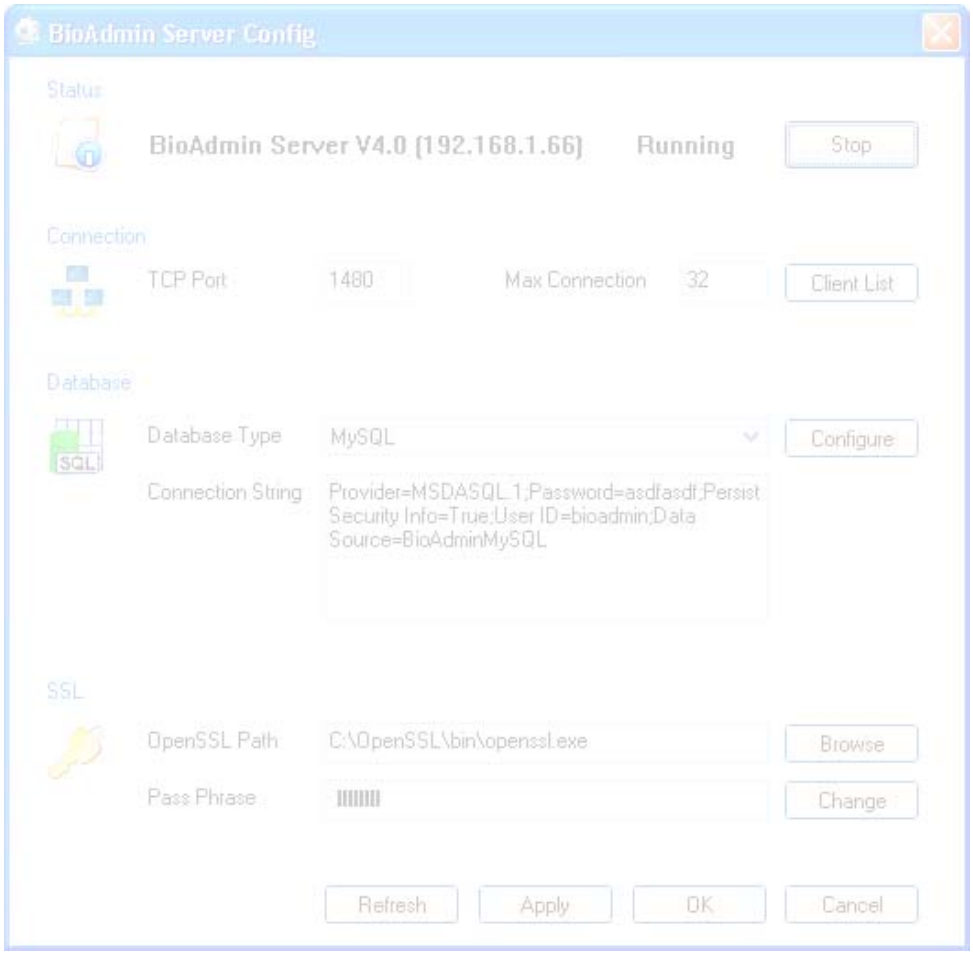
- Press **Test Connection** button to check the connection status.
- Press **OK** button.



- Select the database type as **MySQL**.

- It you were already using the MySQL, press Apply button on **BioAdmin Server Config.** Press **Stop** and **Start** the BioAdmin server.



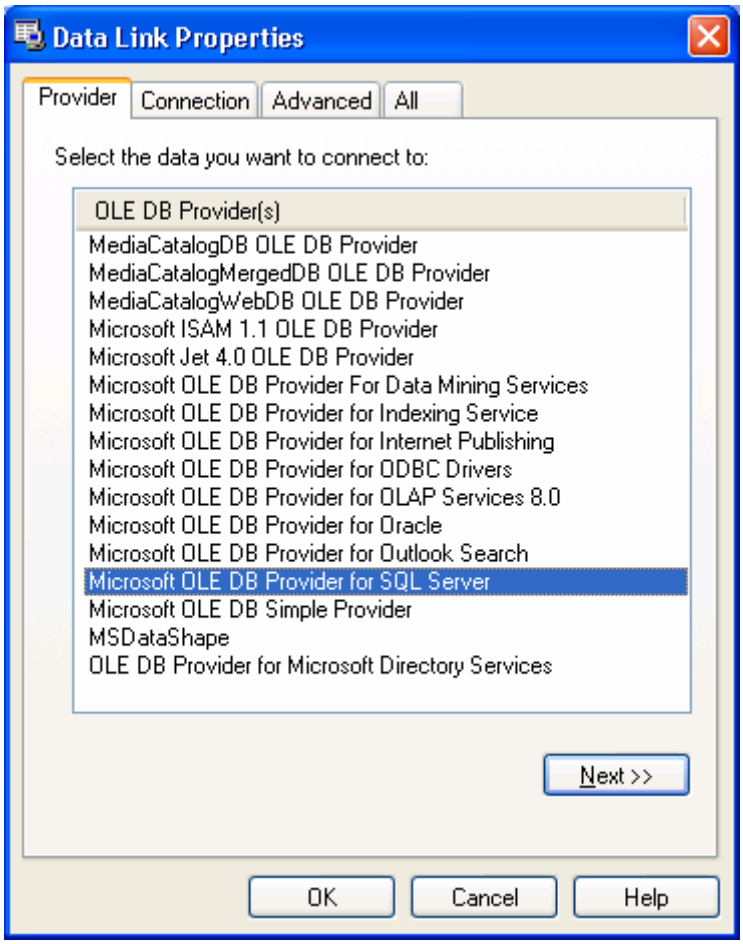


- If the status is changed as **Start**, press **OK** button.

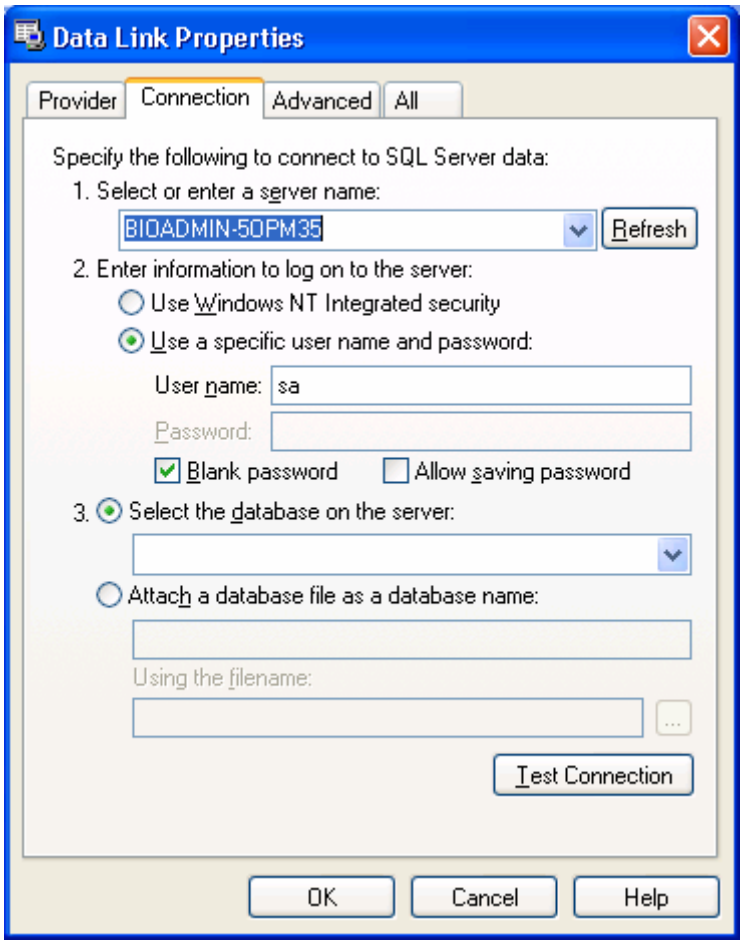
- Using SQL Server database

If you are already using MySql Server, you can use SQL Server database instead of mdb.

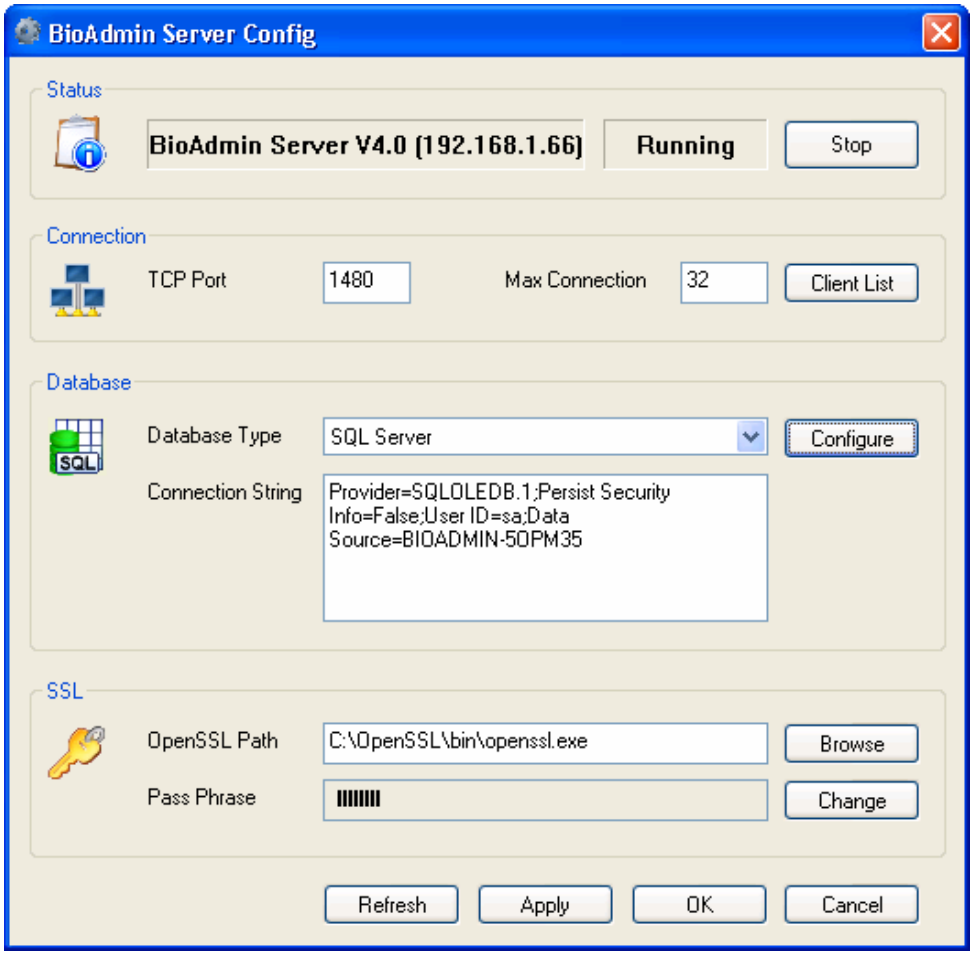
- Execute BioAdmin Server Config menu.
- Click the **Configure** button on the Database field.
- On the **Data Link Properties** window, select **Microsoft OLE DB Provider for SQL Server** and press **Next** button.



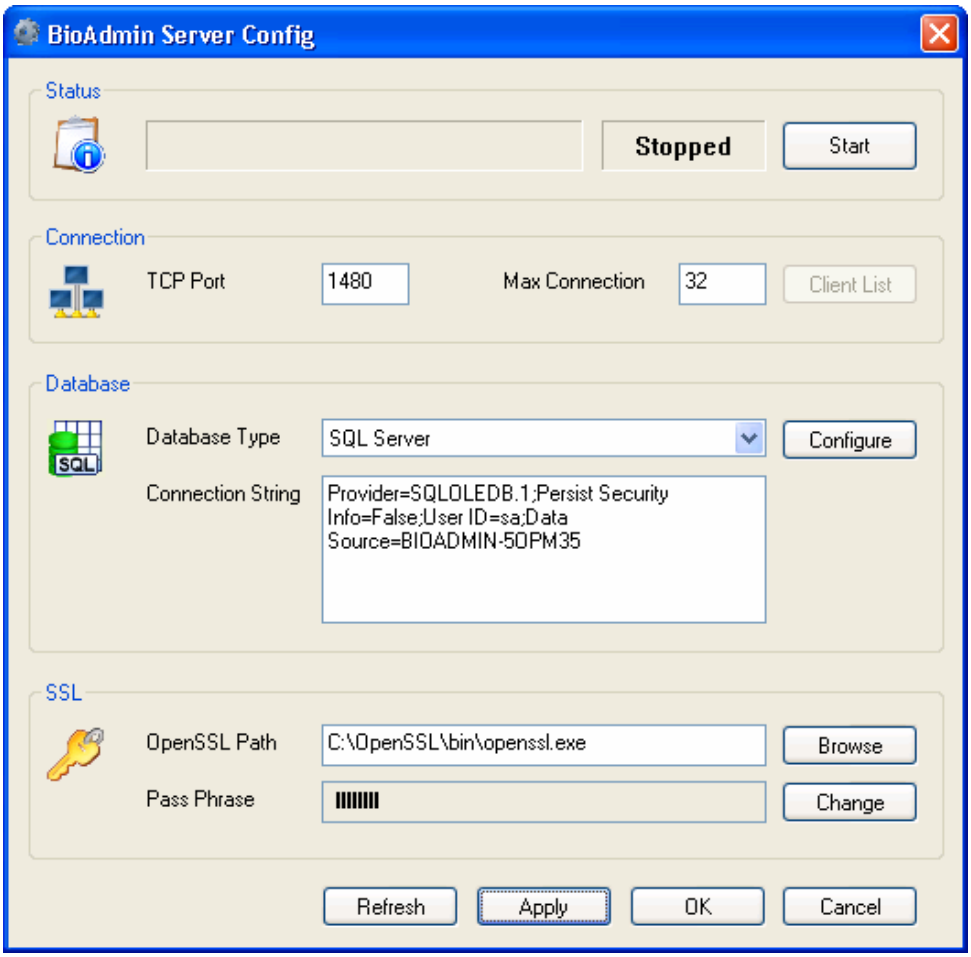
- Enter the SQL Server name.

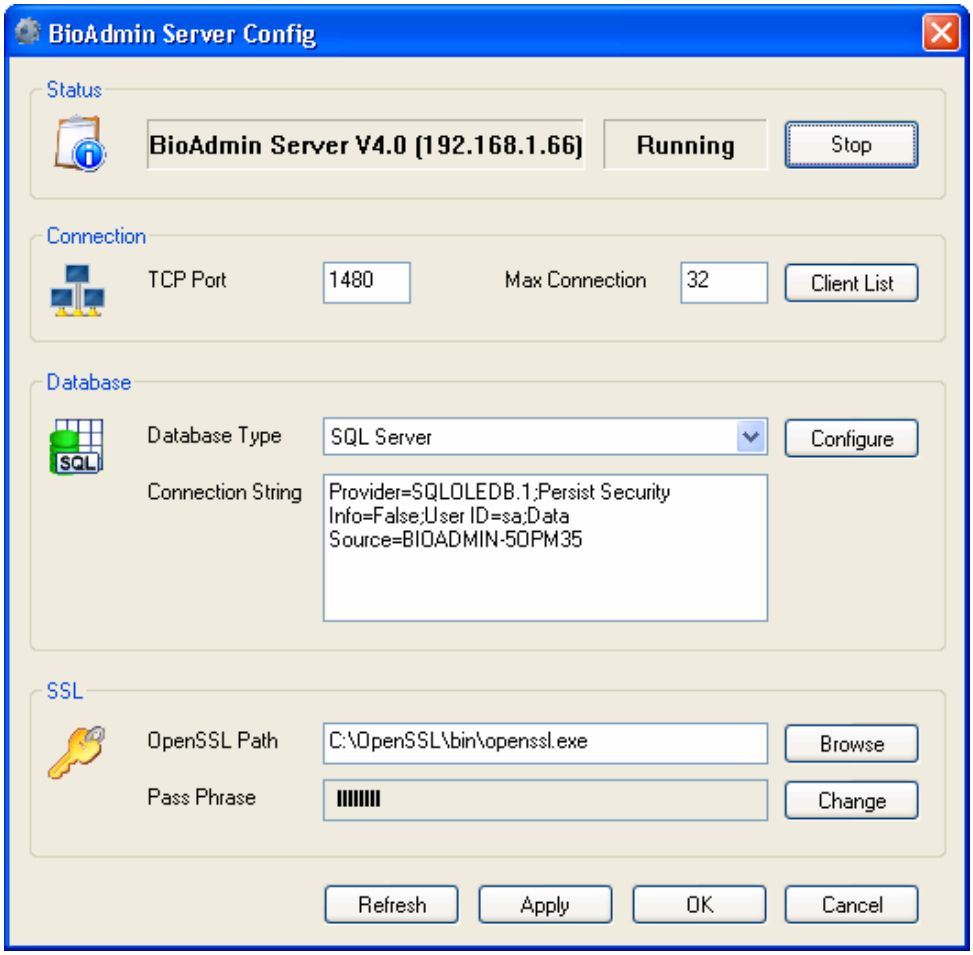


- Enter the User name and Password for the database server. If there is no password, check on the **Blank password**. If there is any password, check on the **Allow saving password**.
- Choose the **Select the database on the server**. To select this option, you should create the database in advance on the SQL Server.
- Press **Test Connection** button to check the connection status.
- Press **OK** button.



- Select the database type as **SQL Server**.
- Press **Apply** button.
- Stop and restart the BioAdmin Server.



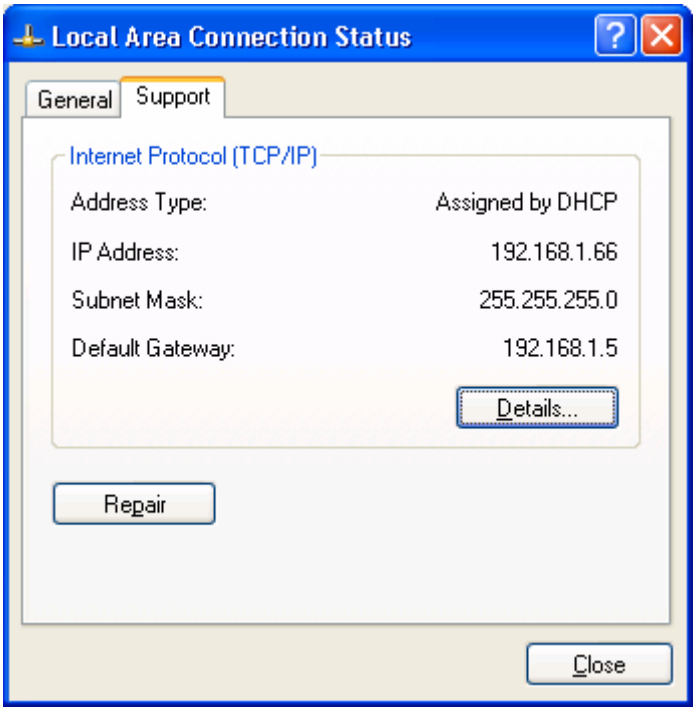


- If the status is changed as **Start**, press **OK** button.

1.4.4. Check the BioAdmin software installation

- Network Configuration

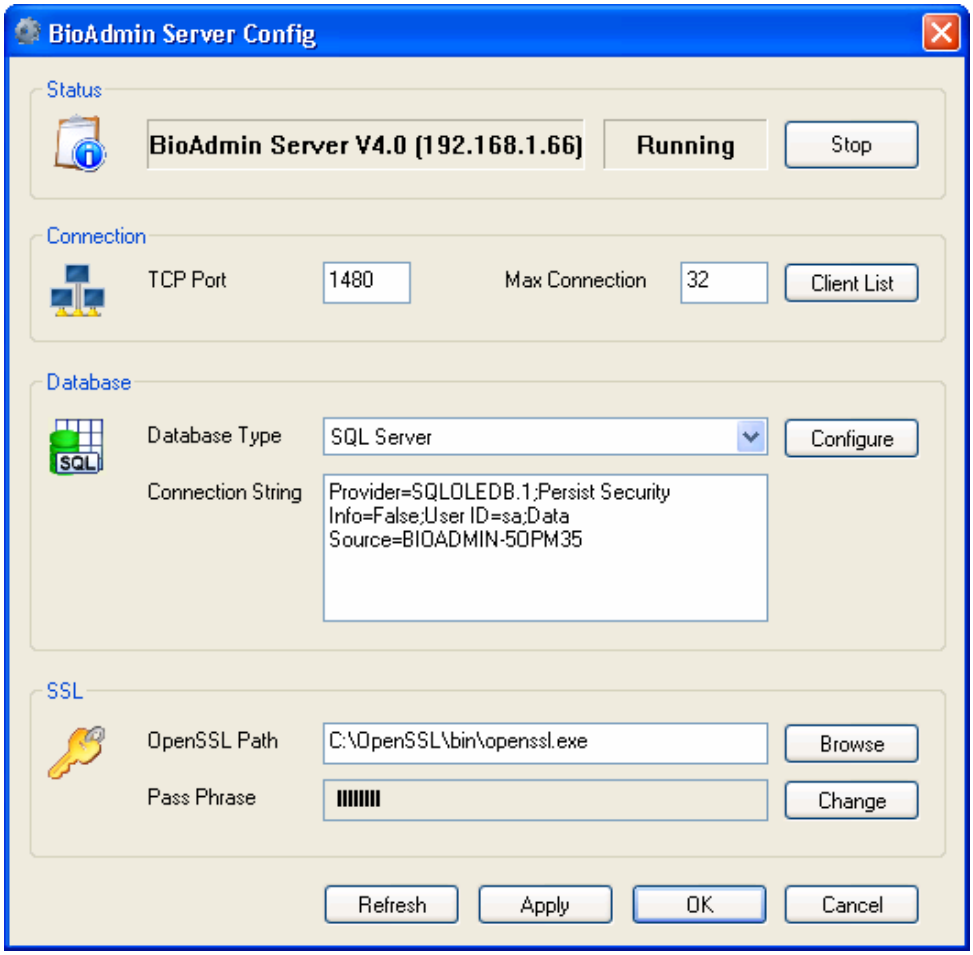
Configure the Network menu of the BioStation as to use the server. Ask the IP address of the server PC to your network manager. You can also check this IP address on Network connection page of your operation system. For more details on BioStation setting, refer to the BioStation Installation Guide.



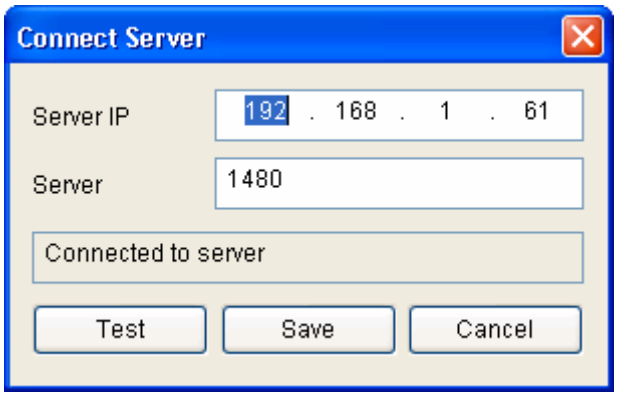
- If you change the BioStation setting to use the server, BioStation will try the connection with BioAdmin Server soon.
- You can check the connected BioStation on BioAdmin Server Config window.
- At this stage, BioStation was just connected to BioAdmin Server, but not managed by the BioAdmin Server. If you issue the certificate, BioStation will get managed by the BioAdmin Server.
- If the BioStation is connected to the BioAdmin Server, BioAdmin Server will get the necessary information from BioStation. This may take a few minutes depending on the data size on BioStation. While receiving data from BioStation, you may not control the BioStation from BioAdmin Client.

● Check Server Status

If you finished the installation of BioAdmin Server and BioAdmin Client, you can check the server status on BioAdmin Server Config window.



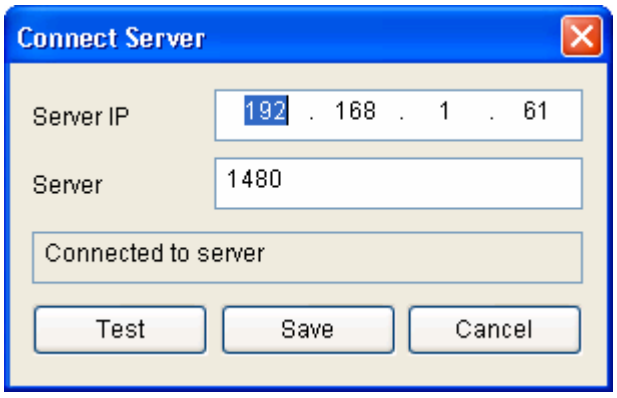
- Check the version and status of the BioAdmin Server.
- Enter the server IP and server port on BioAdmin Client.
- You can check the connection status by pressing **Test** button.



- If you can access to the BioAdmin Server, now you are ready to use the BioAdmin Server and BioAdmin Client.

1.5. Log in to BioAdmin

1.5.1. Connect Server

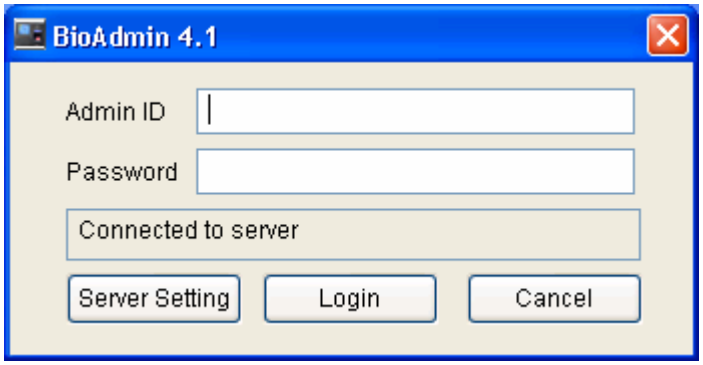


- Enter the server IP and server port.
- Press **Test** button and check whether the BioAdmin Client can access to the BioAdmin Server.
- Press **Save** button to store the server setting and access to that server.

1.5.2. Registering the initial system administrator account

- After entering Admin ID and password, press OK button. At this initial registering, you can put any Admin ID and password.
- This initial registration is required to open the BioAdmin Client program after installing the BioAdmin Server. Therefore, once you register this initial Admin ID and password, you can log in to the BioAdmin Client without registering additional admin account from the next time.

1.5.3. Log in to the BioAdmin 4.1



- After entering the Admin ID and password, press log in button.
- Enter the Admin ID and password you used upon registering the initial administrator account.
- You can see the server information by pressing the Server Setting button.

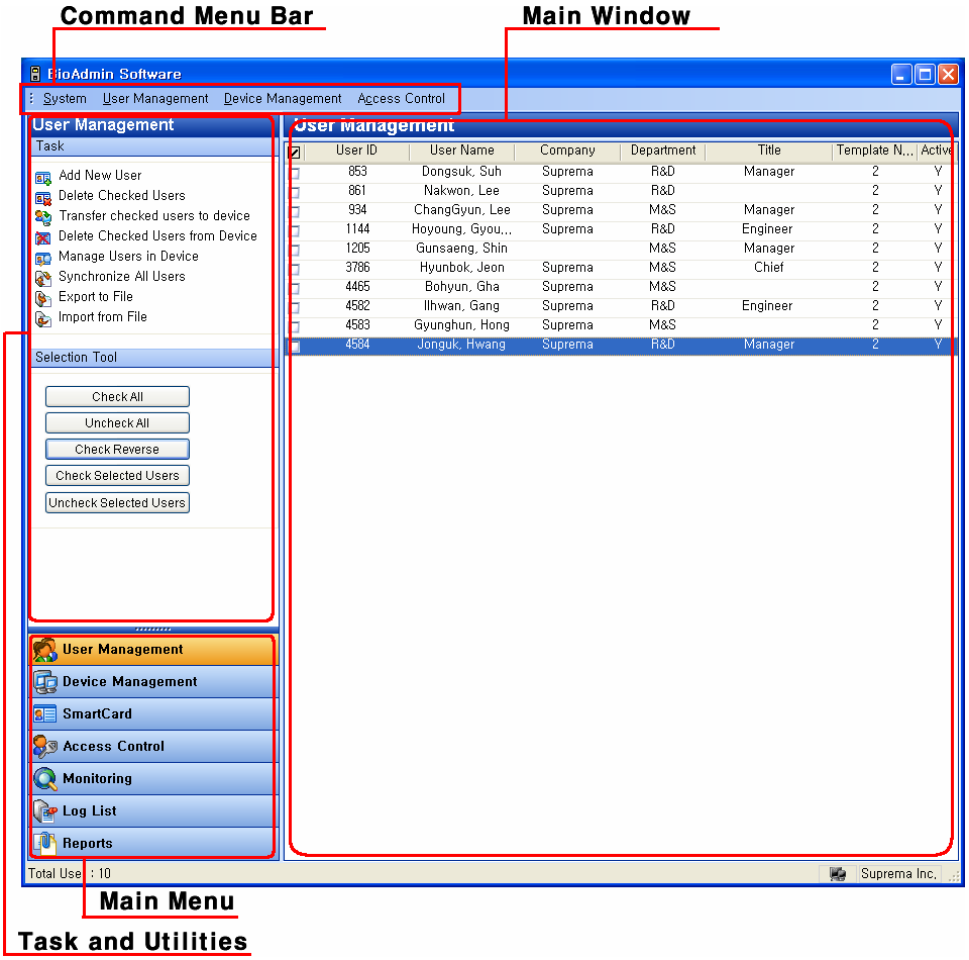
1.6. User Level on BioAdmin 4.1

On BioAdmin 4.1, you can differentiate the user level into three groups as below.

- Administrator : Administrator can change and see all the settings on BioAdmin software.
- Viewer : Viewer can see the settings, but can not change any settings on BioAdmin software.
- User : User can see his log information.

1.7. BioAdmin configuration

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



1.7.1. Command Menu bar

Command menu bar contains command items supported by BioAdmin software, which are grouped into 4 categories:

- System : admin. Account, back up database, restore backup, lock all devices, unlock all devices, upload 1. x version data, preference, BioAdmin information, and close
- User management : add new user, company management, department management, title management, and setup custom fields.
- Device management:: add new device, add new BEACon, set time, upgrade

firmware, upload password initialization code/ password initialization, site key setting

- Access control : time code definition, holiday definition, time zone definition, door zone definition, and access group definition.

1.7.2. 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, log list, or report.

1.7.3. Task list and tool list

Task window shows sub-menus for the selected main menu

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

1.7.4. 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 device
- Information stored on host PC, such as user database or log data
- Controls to manage or to configure the information

1.8. User Database

User database refers to the entire user information including user ID, user name and fingerprint information. BioAdmin software is based on user database management in priority.

That is, user database is created, updated and saved to host PC. Then, it is selectively distributed to BioEntry and BIoStation devices connected to network via transfer.

Note : Difference between select and check – select is used when choosing each user ID in select tool box (press Shift button and choose a user with an arrow key ↓ or click the last user ID with a mouse, to select multiple users.), whereas, check is to check each selected user ID. Using check tool, you can check all, uncheck all, reverse check, check user and uncheck a selected user with ease.

2. Quick start

This chapter explains basic procedures of operating BioEntry and BioStation device integrated with external system.

2.1. Quick start with BioStation

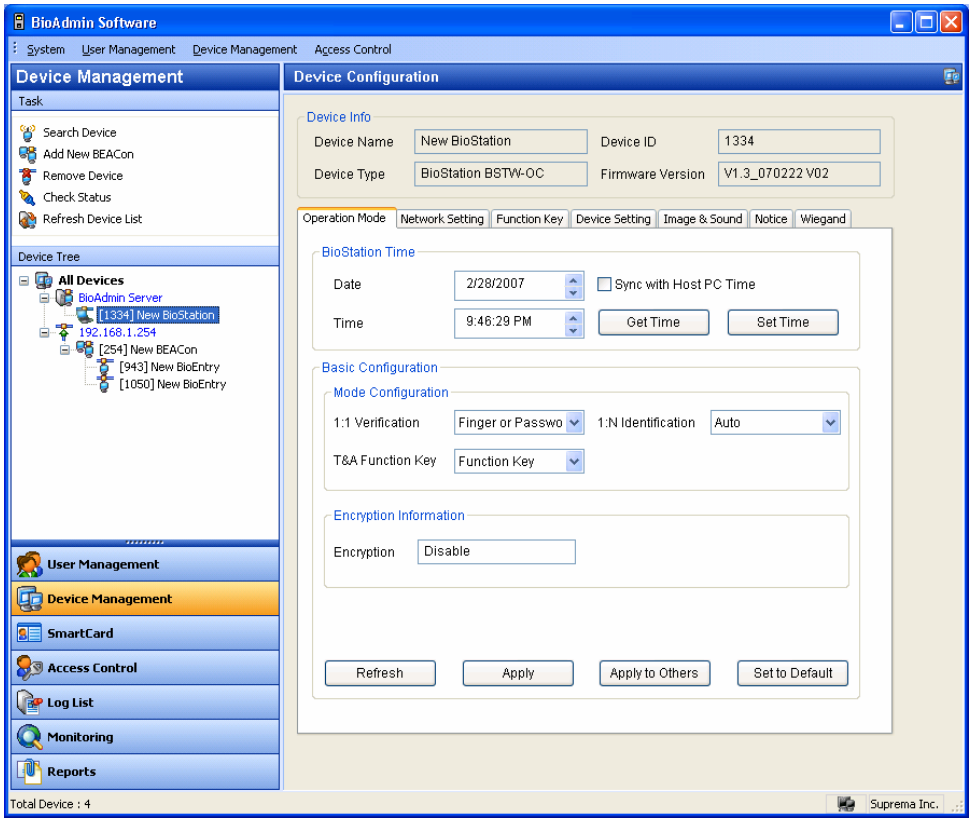
This paragraph describes basic procedures of operating BioStation.

2.1.1. Step 1 : HW installation

BioStation can be networked by cable/wireless LAN as well as by RS232,422,485. Also, BioStation can be use with host PC via USB interface. For details on installation, refer to BioStation installation manual.

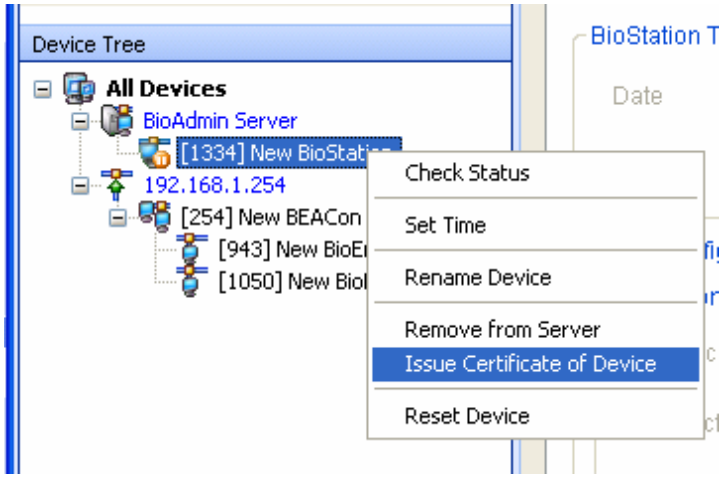
2.1.2. Step 2 : Search new device

- Run BioAdmin software.
- Enter login ID and password.
- Select device management on main menu to display device management page on main window.



- Once the BioStation is connected to the BioAdmin Server, connected BioStation will be added to the device tree whenever you start the BioAdmin software. Also, you can see the connected BioStation by pressing the **Refresh Device List**. Even though a BioStation is properly connected to the BioAdmin Server, it may take several minutes to show up on the device tree.

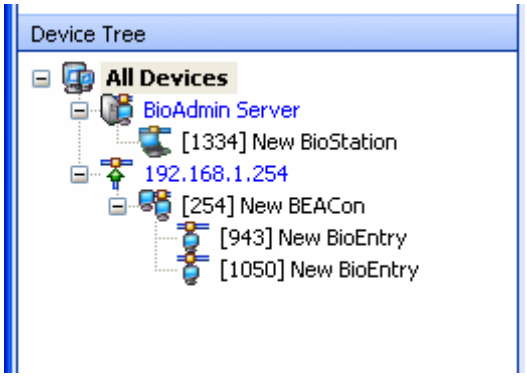
- If a BioStation is unauthorized one, an orange color is indicated on the BioStation icon. In this case, you can not communicate with that unauthorized BioStation.



To communicate with the BioStation, select the unauthorized BioStation and press the right button of the mouse. Press **Issue Certificate of Device** menu. After issuing the certificate, you can use this BioStation.

Because the BioStation restart after issuing this certificate, it may take a few minutes to show this BioStation again on the device tree.

- After the certificate is issued for the BioStation, orange mark will be removed from the BioStation icon. This means that you can communicate with the BioStation without any problem.



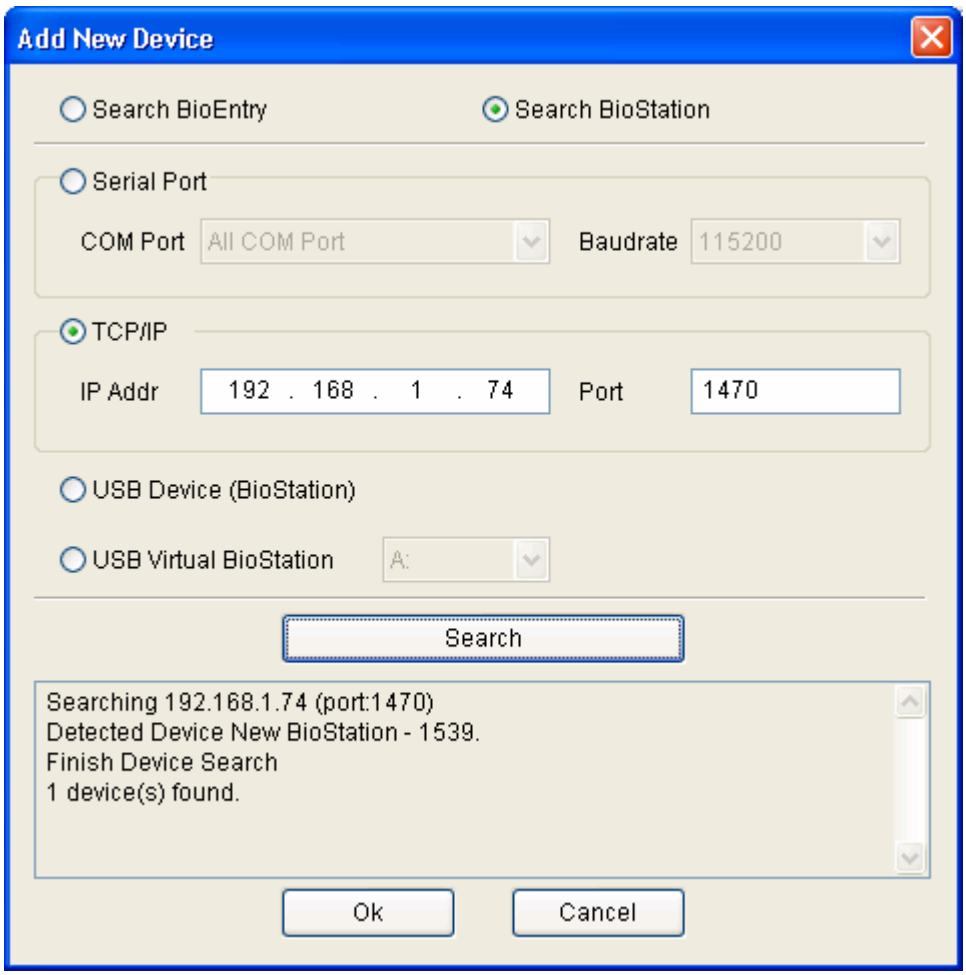
- Select Search device menu, click BioStation search, select a desired network out of serial port TCP/IP and USB device (BioStation) and press search button.

Note : If you find a device from search results Ex.) searching 192.168.1.101 (port : 1470),

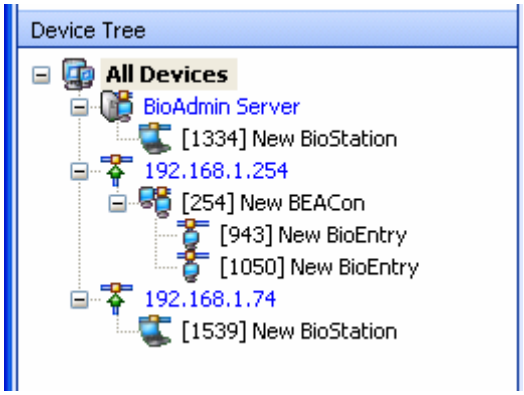
Detected device : new BioStation – device number

Finish device search.

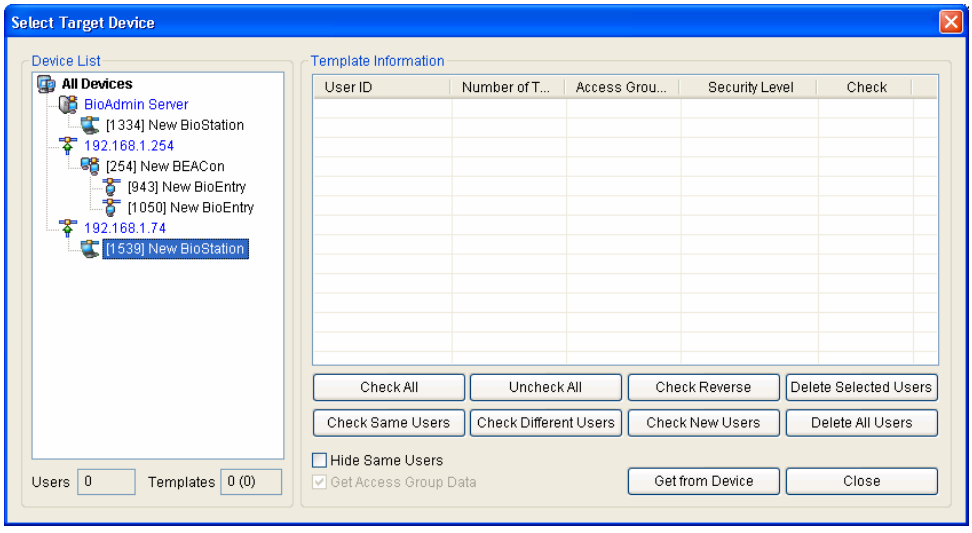
Search result '---- device(s) found' is displayed. Press OK button to select a ,device.



- Once it's connected to device successfully, new device ID and network connected to device are also displayed in device tree window.



- Select user management button on main menu and select Manage users in device on task window.
- Once device is selected, fingerprint information such as user ID, number of fingerprint, access group, security level and select is displayed.

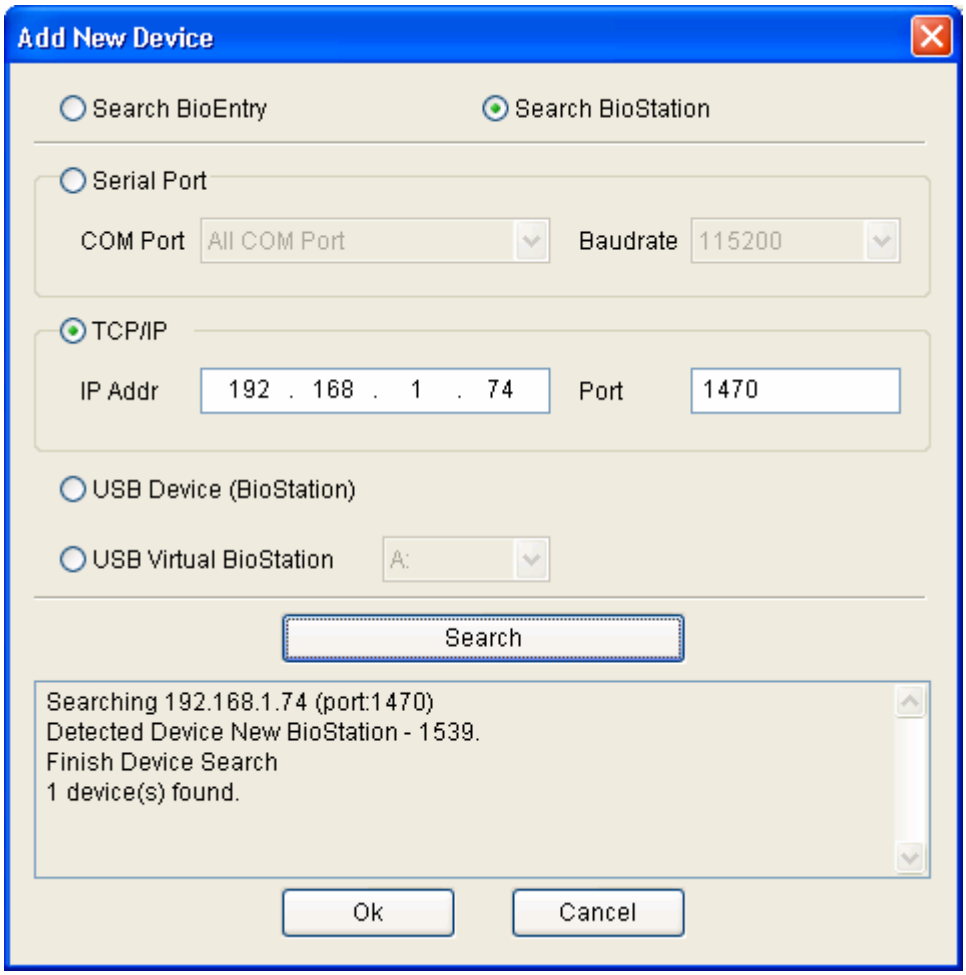


2.1.3. Step 3: Connect device

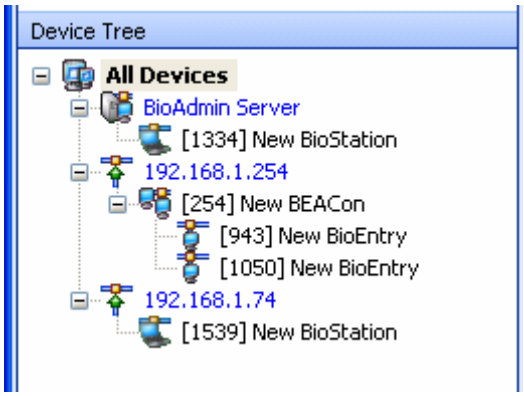
- Select Device Management menu to display device management page on main window.

  BioAdmin software network setup is divided into network, serial port and USB connection. Change settings and apply them to device.

  Network setup is to designate settings for local and wireless network connection. You need to designate the port as “1470.”



Administrator needs to know IP address and port # (1470). Once device is connected properly, IP address is displayed as one group and device ID is displayed with a bracket [****] on device tree window.

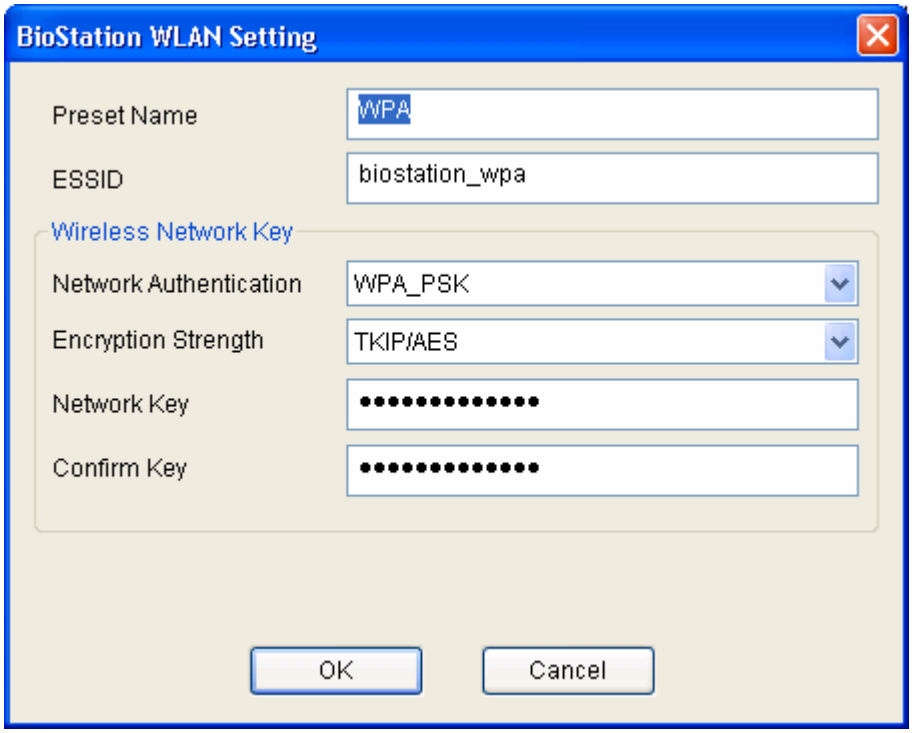


- Wireless network setup

Set up free set name, network name (SSID), data encryption, key type, and network key check on wireless network setup before operation.

Applying DHCP, you can set automatic upload of IP address on BioAdmin in order to get IP address automatically, check such an IP address and search a device in device management.

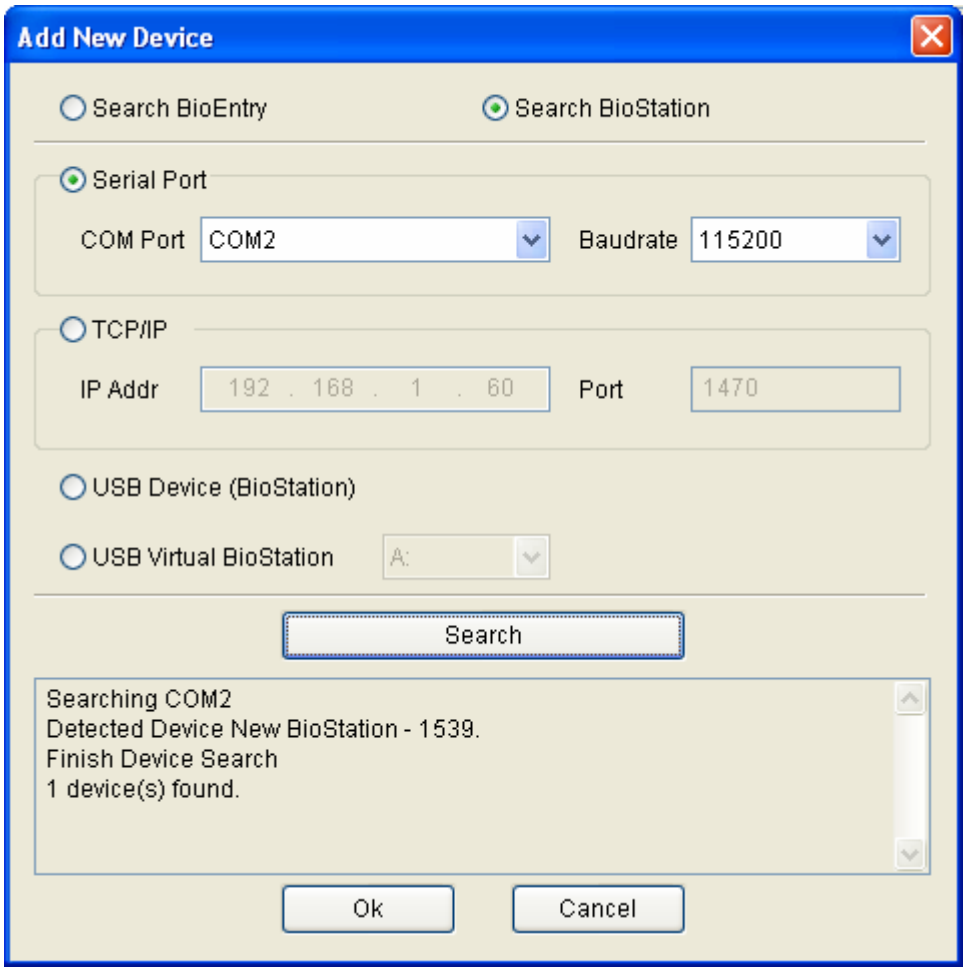
When setting IP address manually, you can search a device by specifying assigned IP address, gateway and subnet mask.

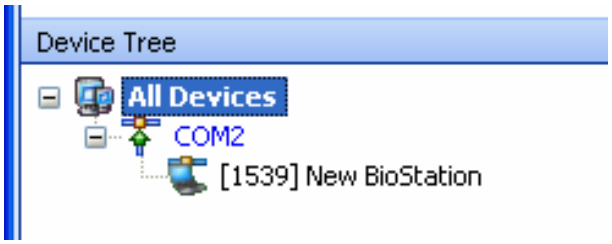


- Serial

On RS422/485 network, a new device can be detected automatically or added by new device search menu in device management. Once device is connected to network properly, device ID will be displayed with a bracket [****] under port on device tree window.

Baudrate in RS485 / RS232 interface represents the frequency of carrier wave changing status per sec. In communicating with BioStation device, default is 115200 but if any trouble, lowering the baudrate can solve the problem.





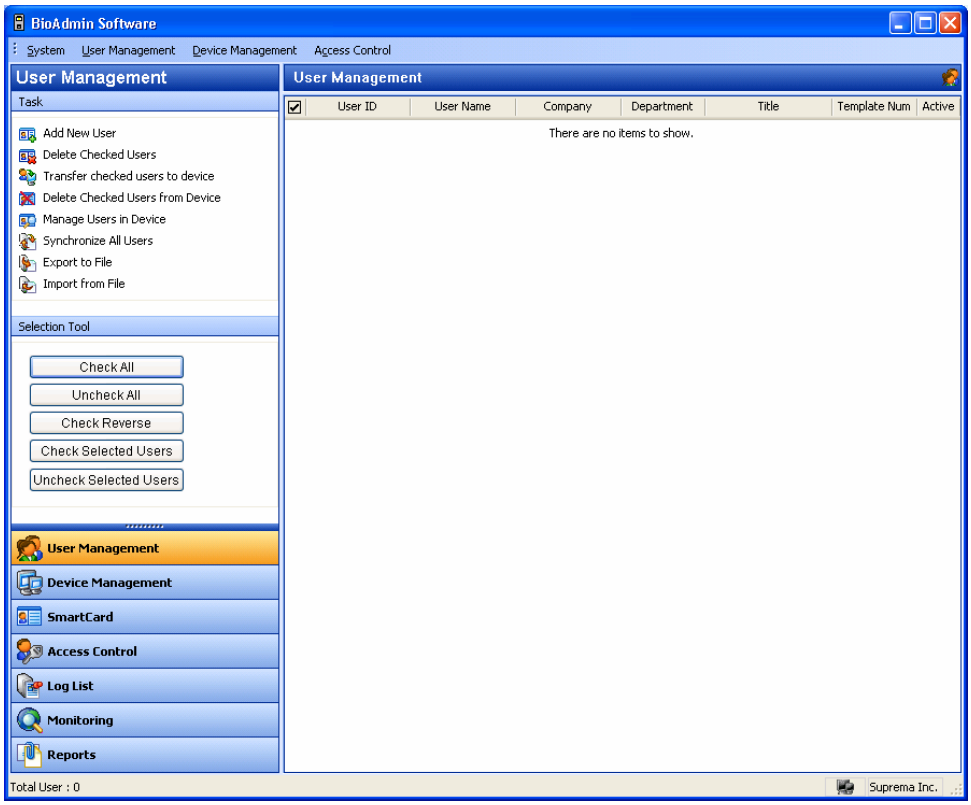
Although a device is disconnected from network, it still remains on device tree window. Remove device menu is used when removing a device from device tree window.

Device name can be changed using change device name menu but device ID can't be changed as it is fixed as one.

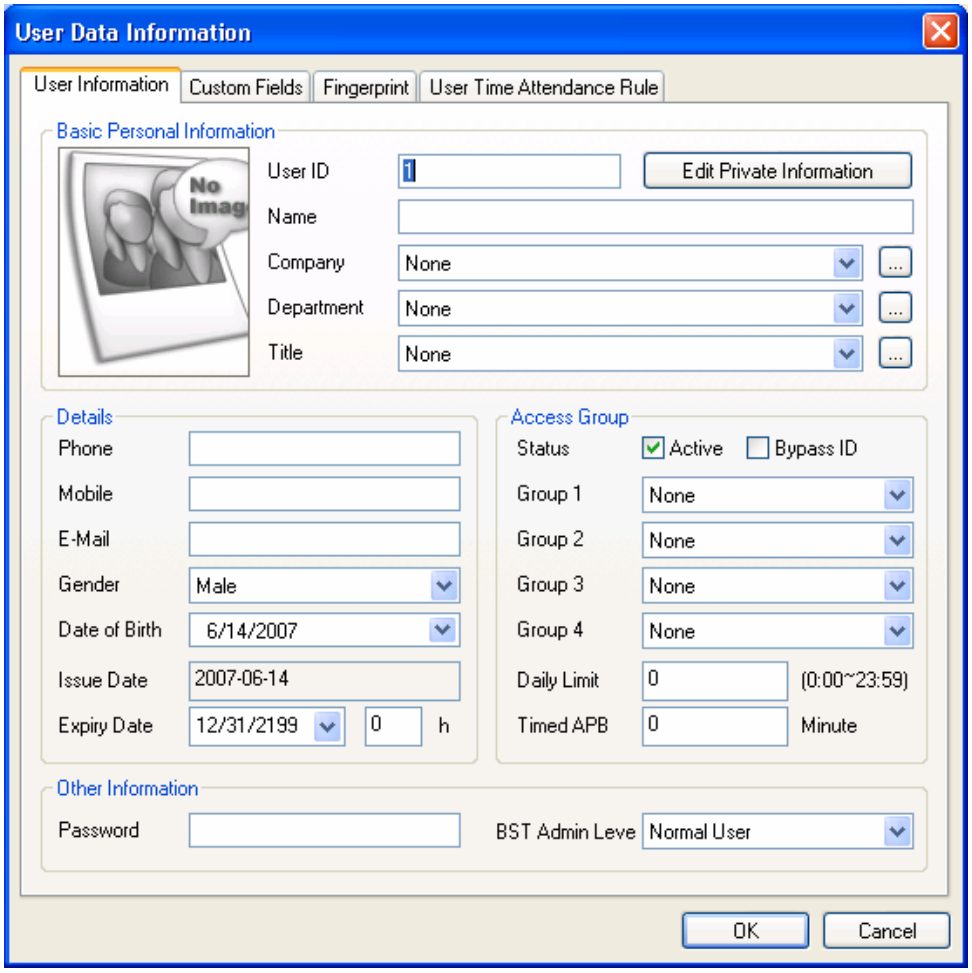
2.1.4. Step 4: User management

- Select user management menu to display user management page on main window.

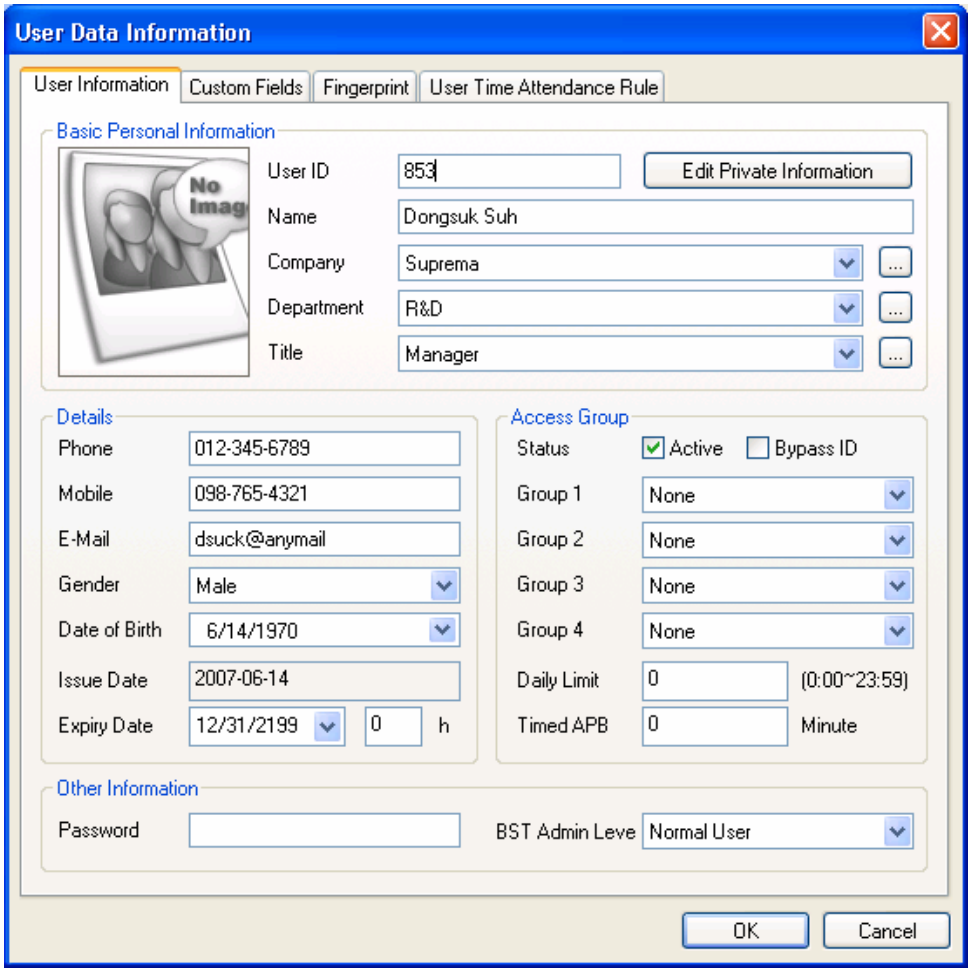
> Note : In user management, user related information can be divided into basic information and fingerprint information. Basic information includes user ID, name, company, dept., position and telephone number. Fingerprint information is about user's fingerprint.



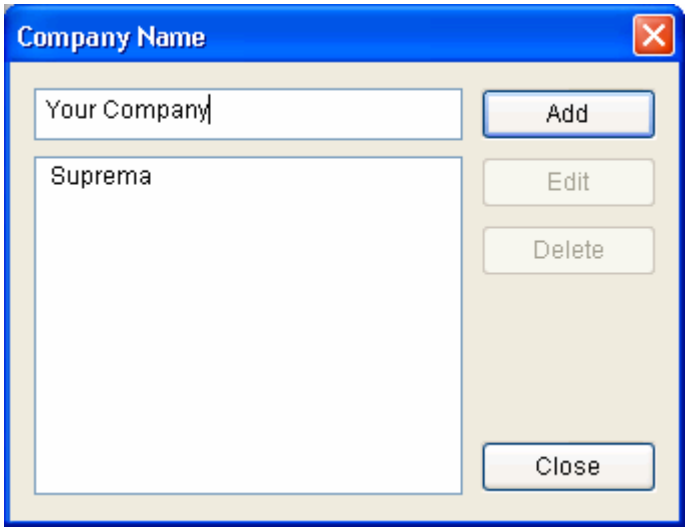
- Select add new user menu on task window to pop up a window.



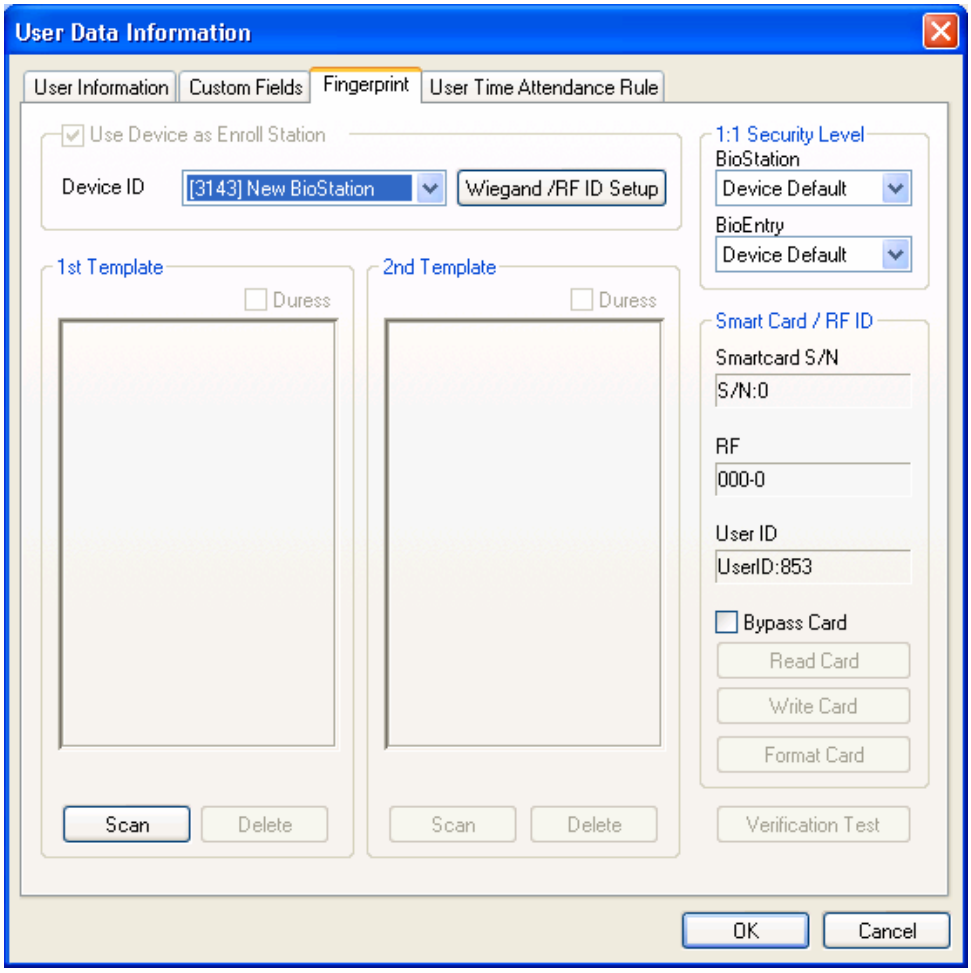
- Click user information tab and enter user information.



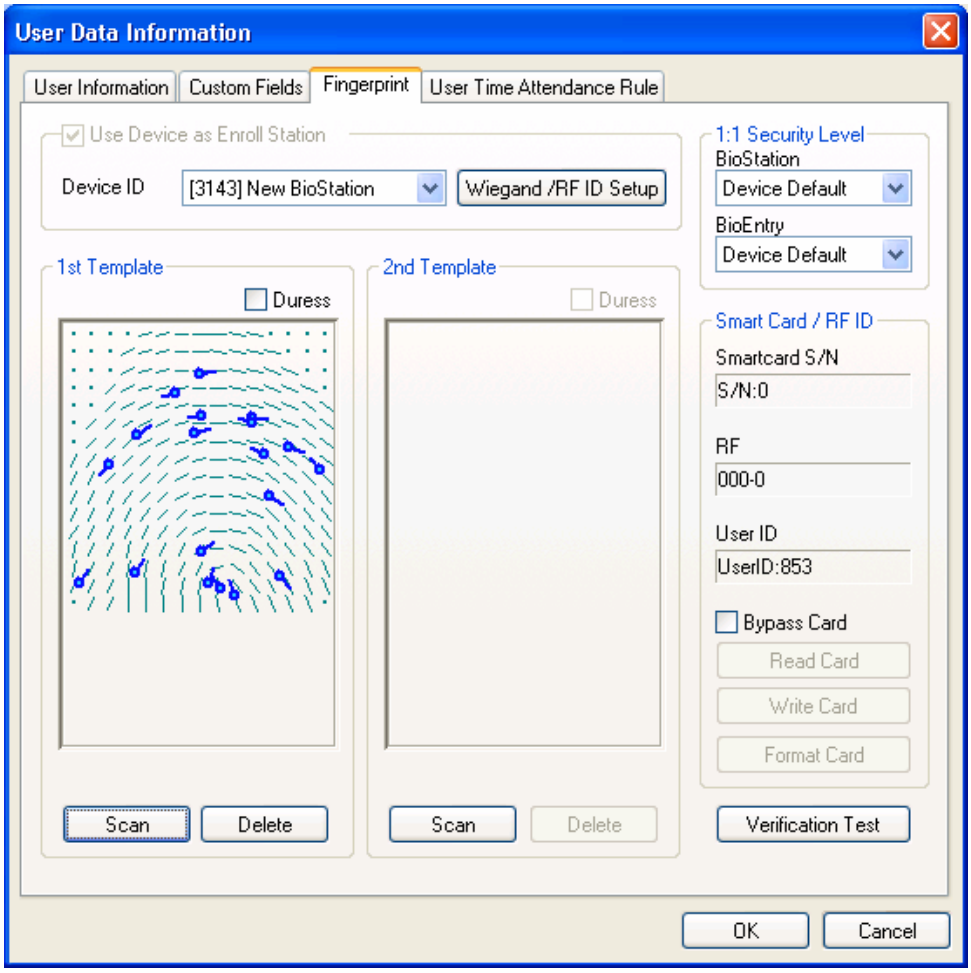
- Choose company, dept. and title using a combo box.
- To add a new company, dept., or title information, press ... button or enter company, dept. or title in information input window and then press add button.
- To save added information, press save button.



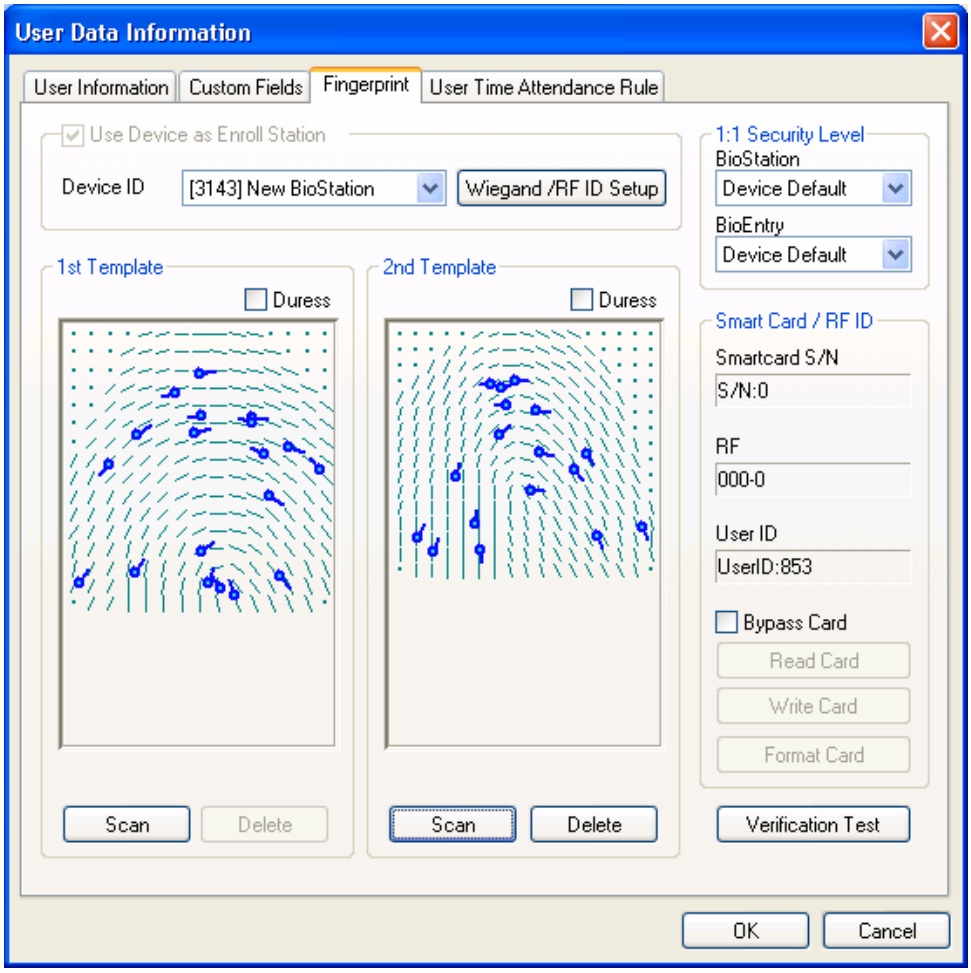
- To enroll user's fingerprint information, click fingerprint tab.
- Fingerprint input process is divided into one by USB fingerprint scanner and the other by BioStation device.
- How to input fingerprint information using USB fingerprint scanner is as follows.



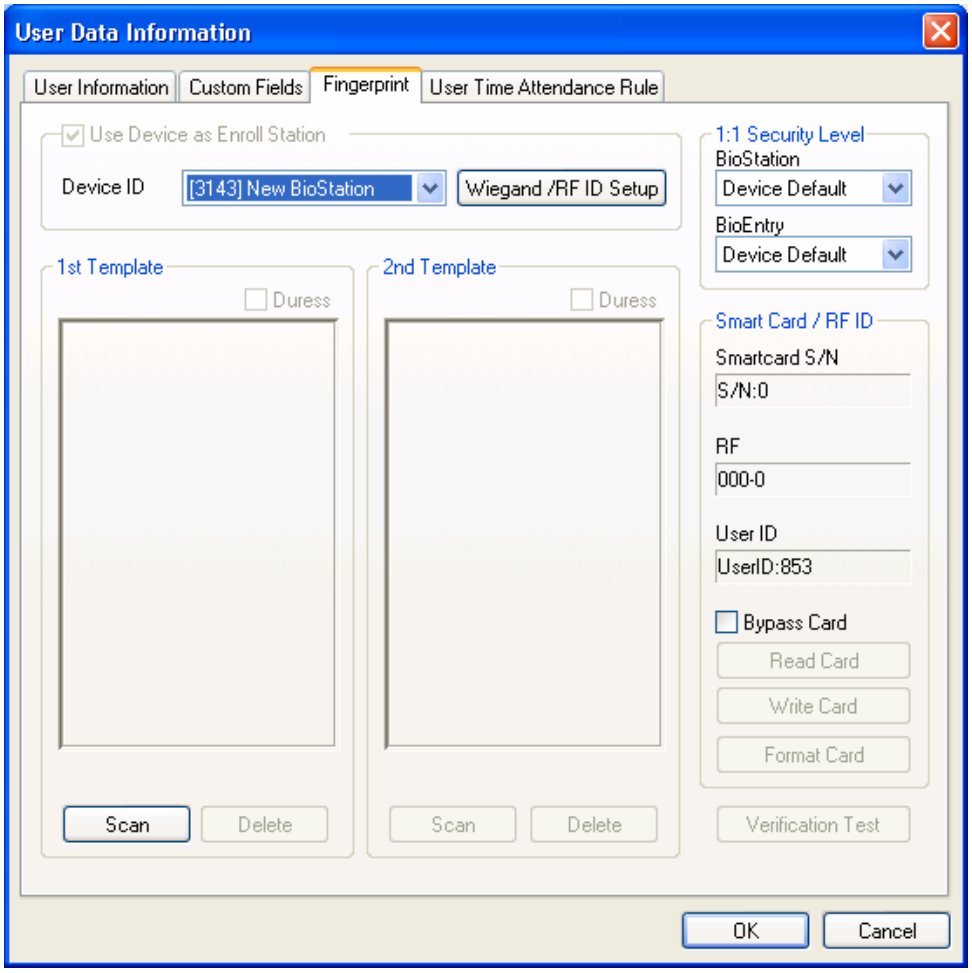
- Press scan button, place a finger on USB fingerprint scanner twice and input the first fingerprint information.



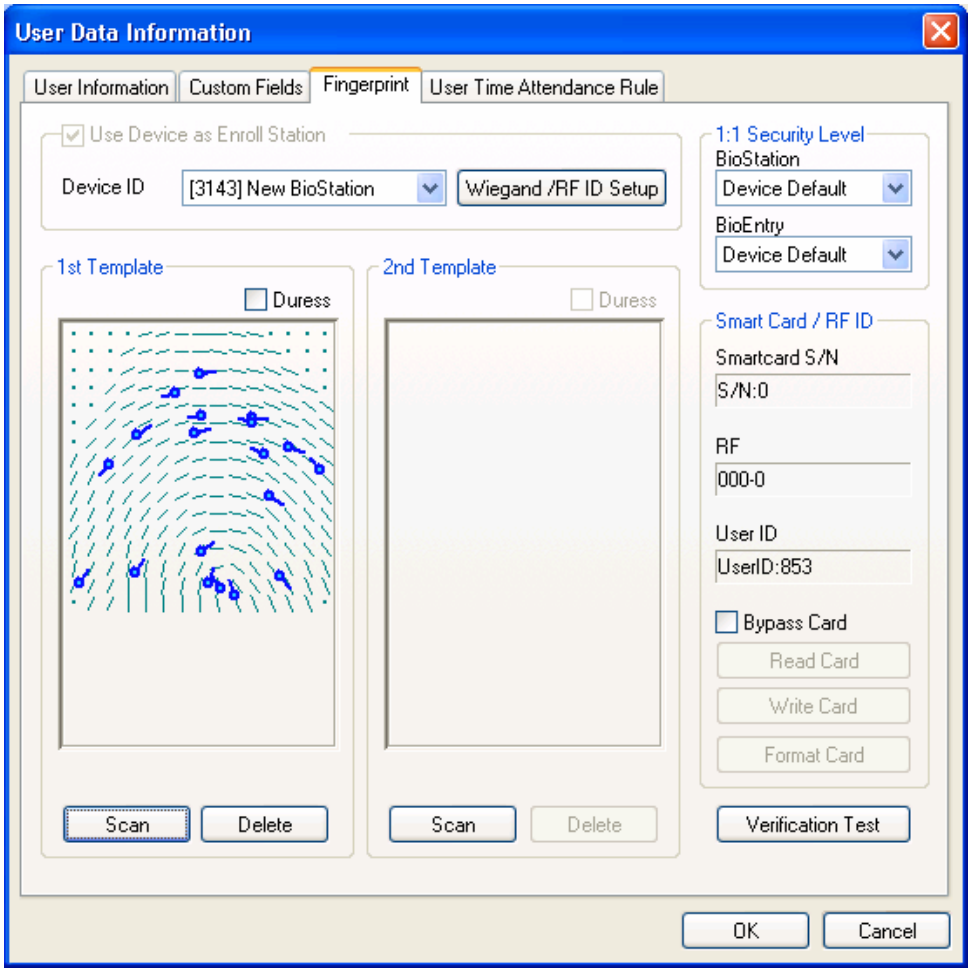
- Input the second fingerprint information in the same way as the first fingerprint information input process.



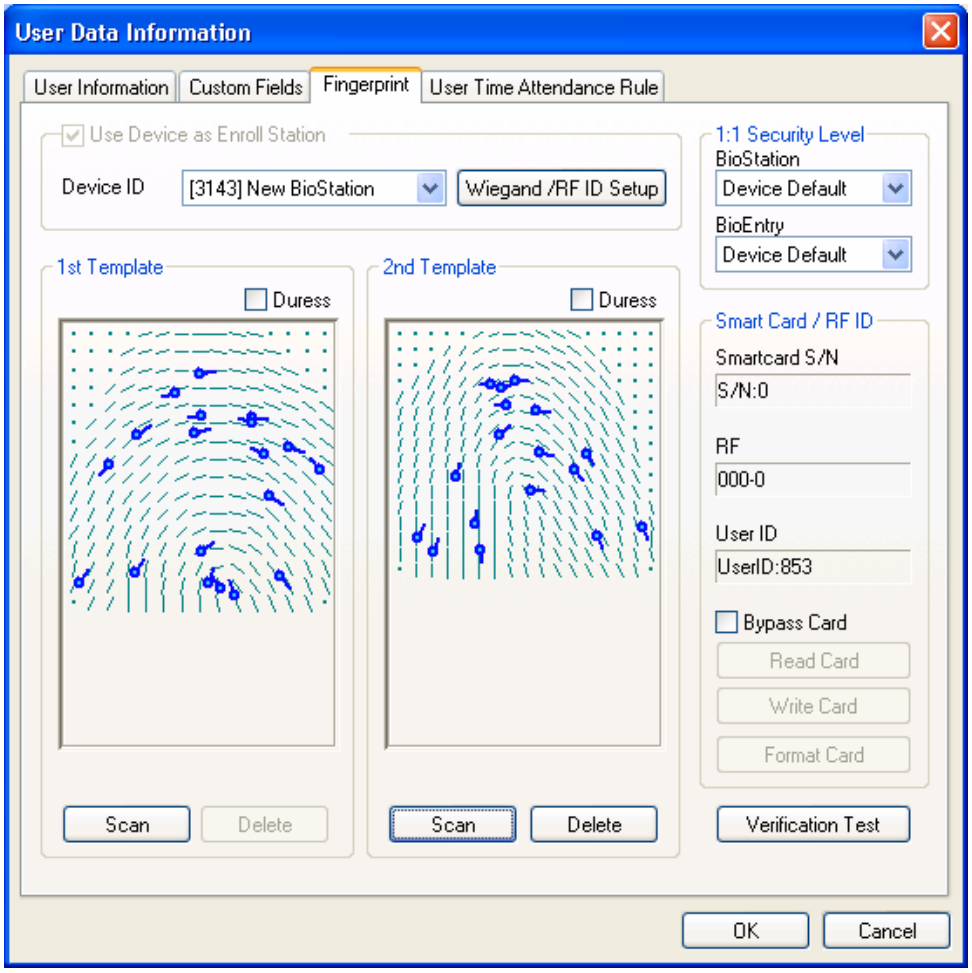
- How to enter fingerprint information by BioStation device is as follows.



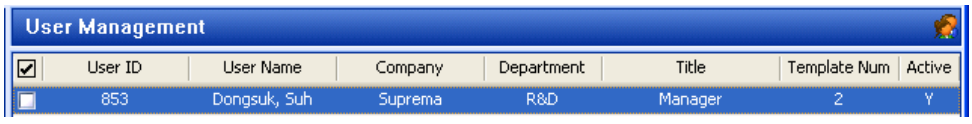
- In case of stand alone mode without USB scanner, check Use BioStation as Enroll Station, press scan button, place a finger twice on device and then input the first fingerprint information. In case that device is configured by 2 or more networks, specify BioStation ID, press scan button, place a finger on device twice and then input the first fingerprint information.



- Input the second fingerprint information in the same way as the process of first fingerprint information input.

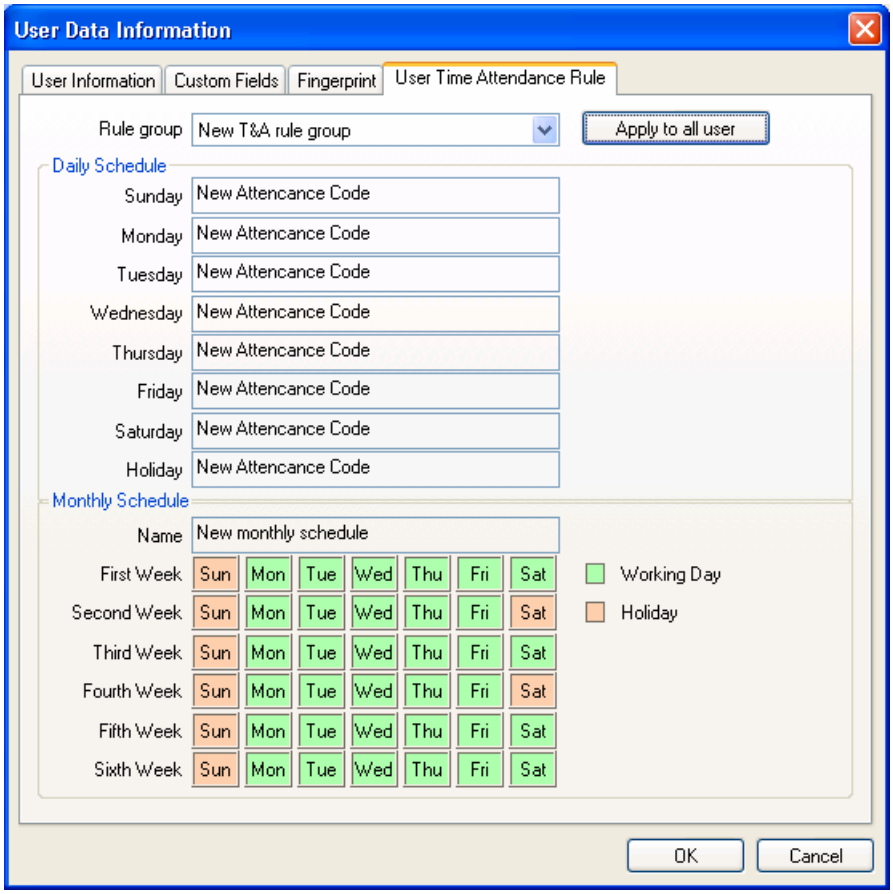


- To close enroll process, click OK button. Then you can see enrolled user information on user list window. This means user information has been added to Database in host PC.



2.1.5. Step 5 : Rules on user T&A event control

New T&A rule can be applied by day.

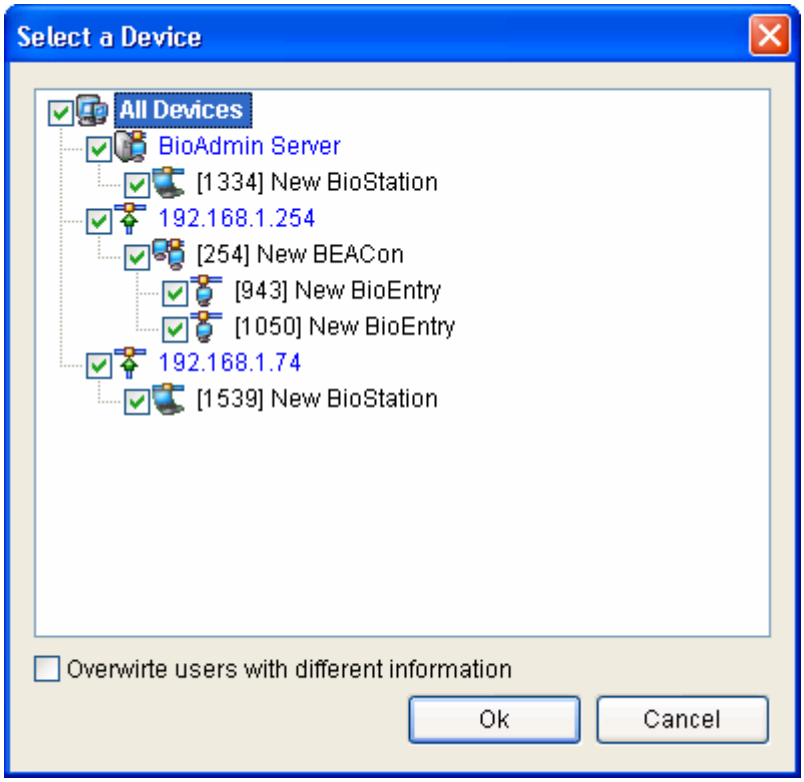


2.1.6. Step 6 : Enroll user with 'transfer checked user to device' menu

Transfer checked user to device is used to transfer user database from host PC to BioStation. User information such as user ID, fingerprint information, access group and security level is transferred through this process.

- Check enrolled user

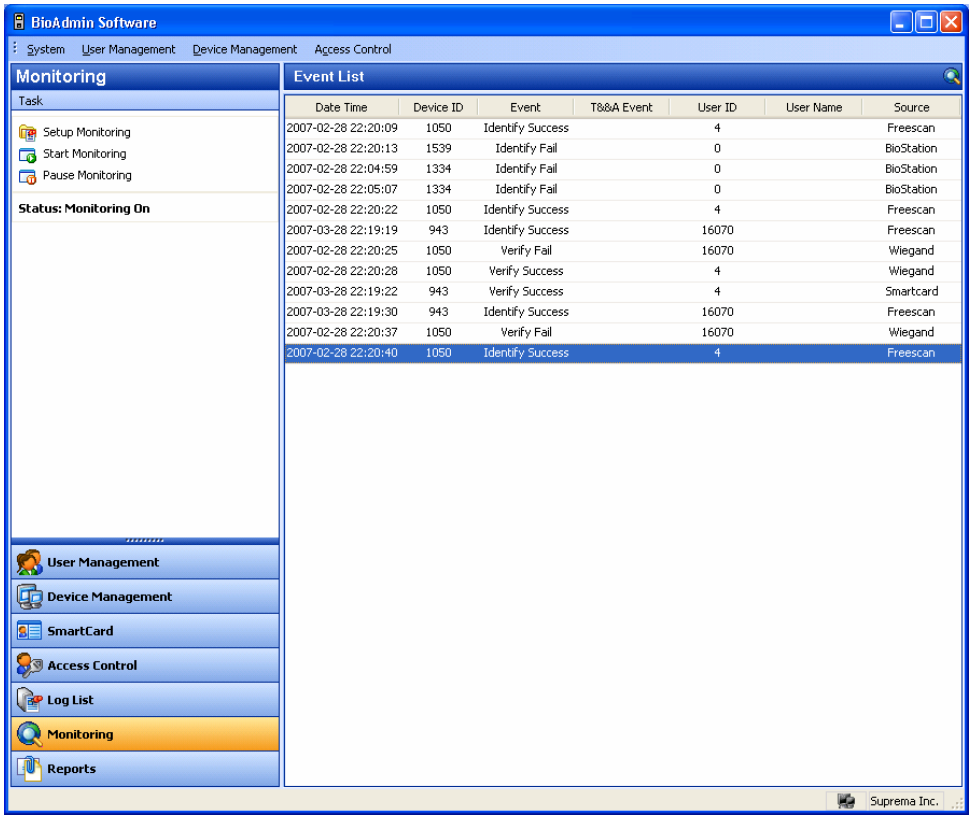
- Click **'transfer checked user to device'**, check **'device'** and click **ok** (select) button.



Press **Manage users in device** button and click device**.** If user information fields are indicated in yellow, it means user information has been transferred to device successfully.

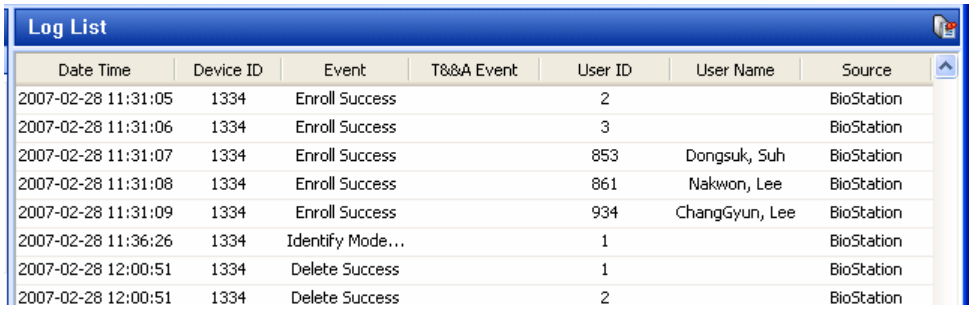
2.1.7. Step 7: Monitoring

- Select **Monitoring** menu to show Monitoring display on main window.
- Select **Monitoring setting** menu and double click Monitoring on/off**.** To save, click ok button. To start monitoring for linked all BioStation devices, select **start monitoring**.



2.1.8. Step 8: Log List

- Select the **Log List** menu. Then, the log list window appears on the main window.
- Select the Get **Recent Logs / Auto Upload** button to see the updated event log data added to the existing log list of BioAdmin.



2.1.9. Step 9: Report

Select report menu to display report list on main window. You can specify company name, dept. name, user ID and user name for setting and select required type of

report such as daily report by setting period or individual report.

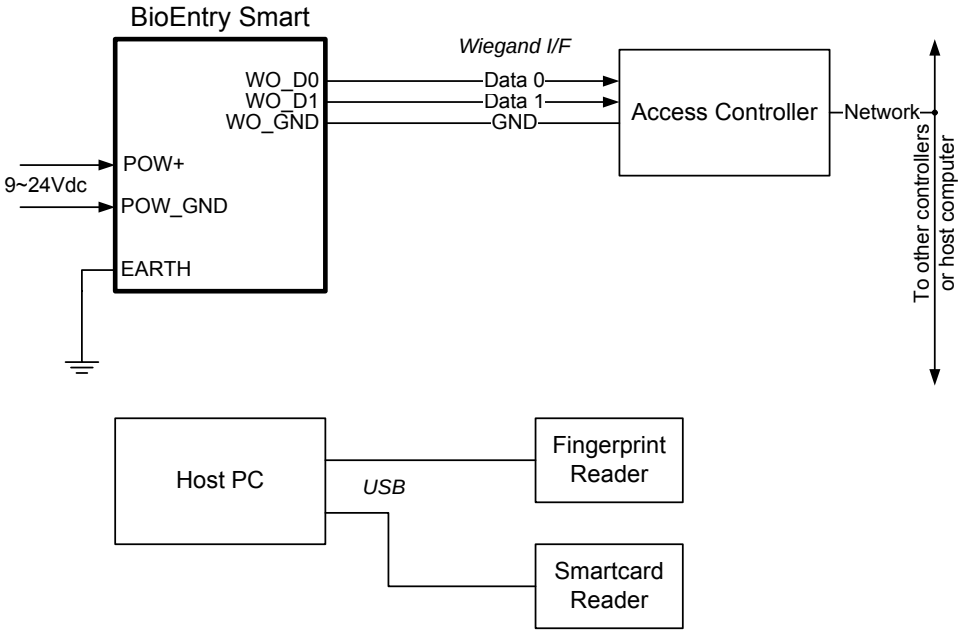
Upload log is a button to upload a log saved in device and **update report** button is a button which implements display prior to output listing a log uploaded device by date and individual. Lastly, view report is a button to preview a report. Press print button to print.

2.2. Quick start with BioEntry Smart

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

2.2.1. Step 1: Hardware installation

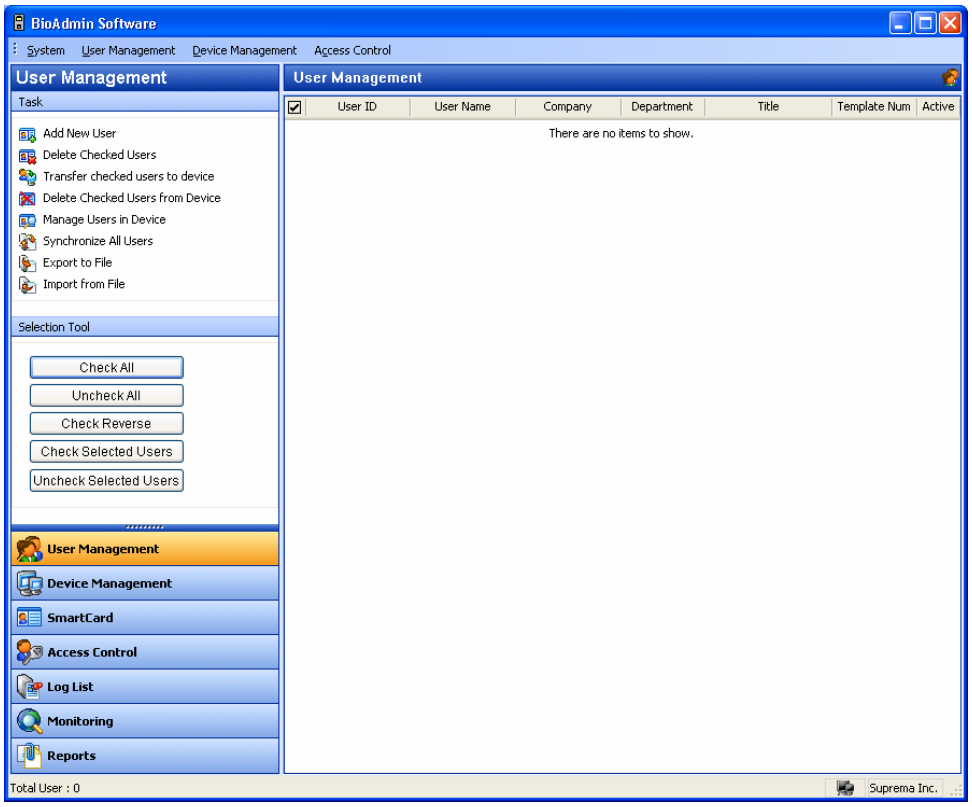
In this hardware configuration, the device is not connected to the host PC, but to an external controller via Wiegand interface. It is assumed that the controller supports the standard 26 bit Wiegand format as default on BioEntry device. Connect the device with the controller as shown on the following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



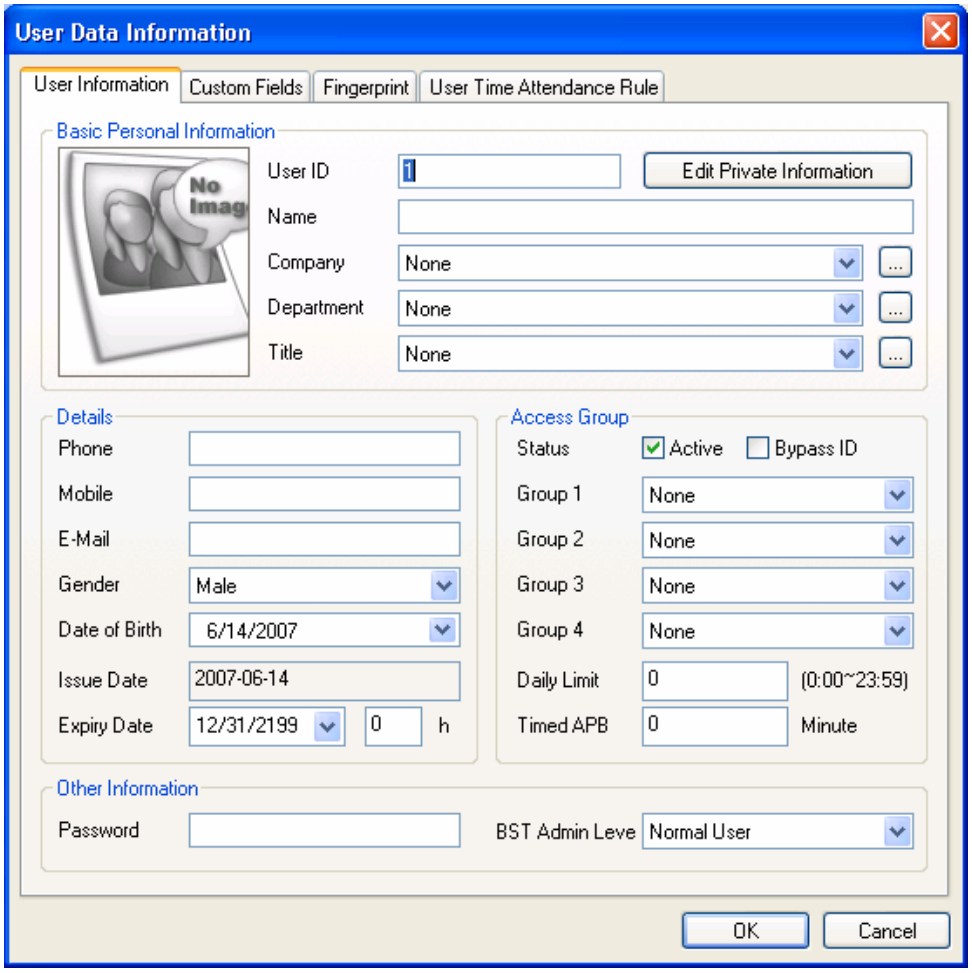
For more details on the installation, refer to the BioEntry Installation manual or BEACon Operation Manual.

2.2.2. Step 2: Enroll user

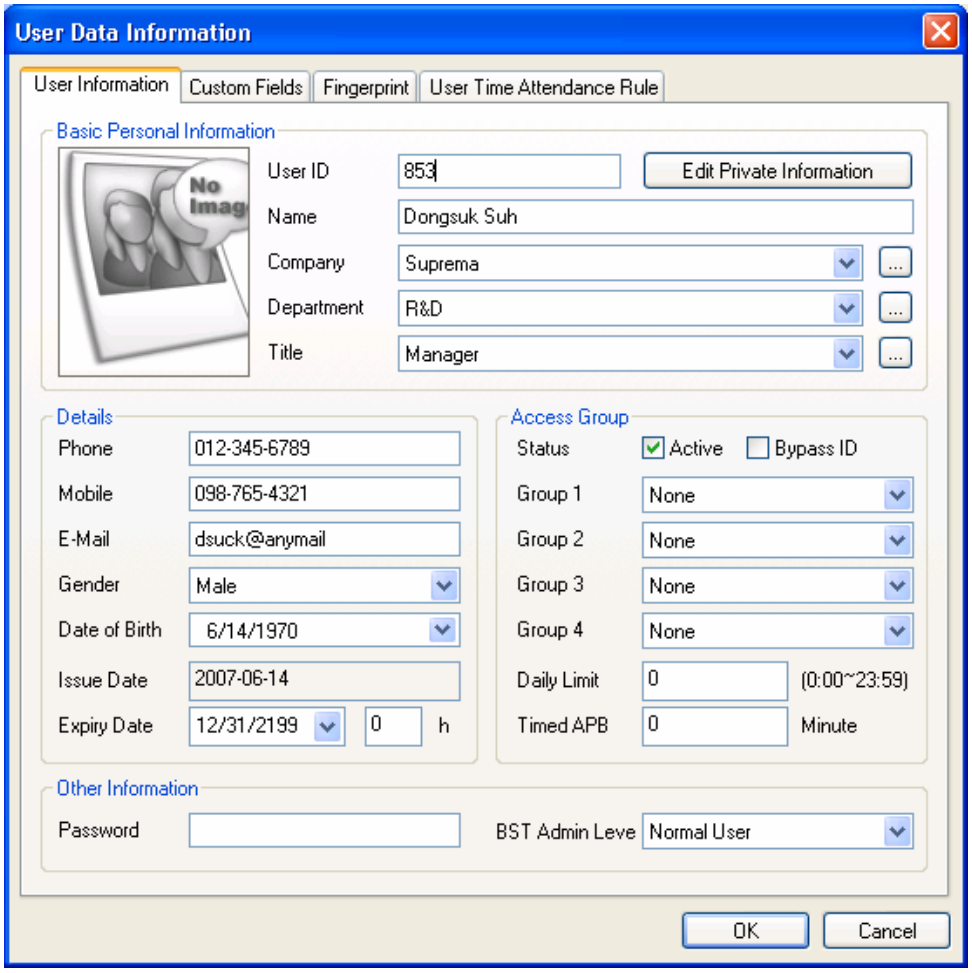
- Run BioAdmin software.
- Enter Login ID and password. By factory default, the initial Login ID is "**admin**" and the password is blank.
- Select **User Management** on the main menu, then the user management page appears on the main window.



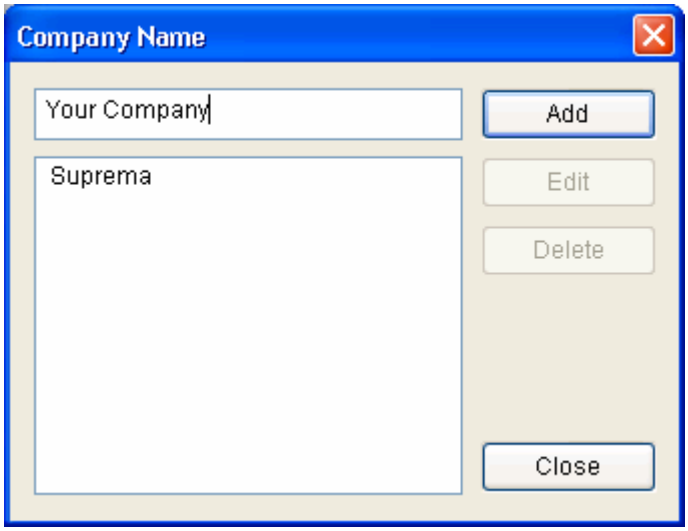
- Select the **Add New User** menu on the task window, then the pop-up window appears



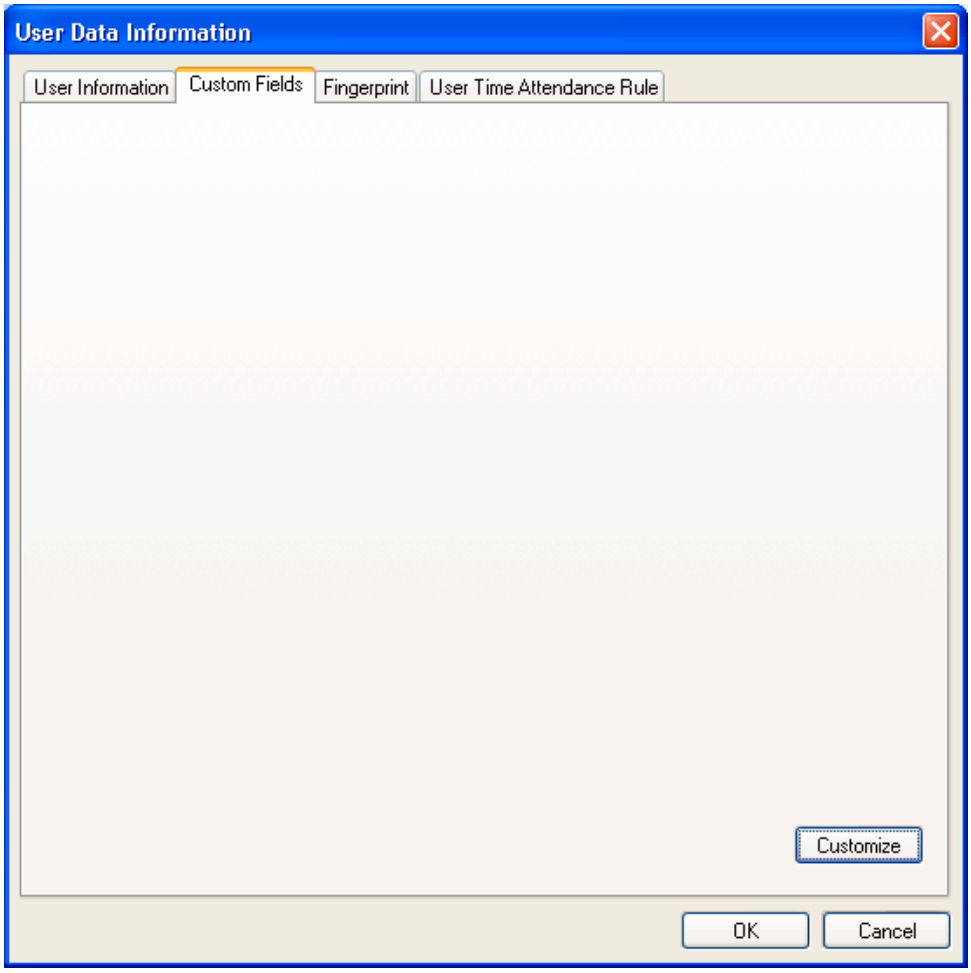
- Enter the u**ser information** on the User Information tab.



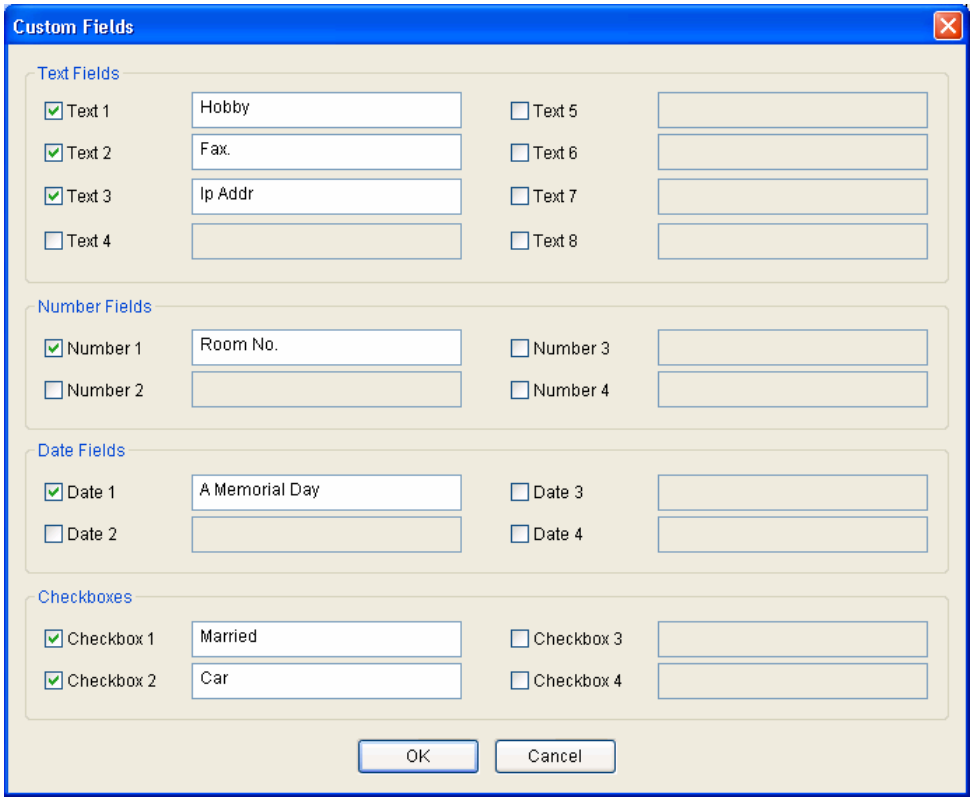
- Especially, you can select the Company, Department, and Title on the drag down menu.
- To add new Company, Department, or Title information, press [...] button. After entering the required information, press **Add** button. Press **Save** button to save the added information.



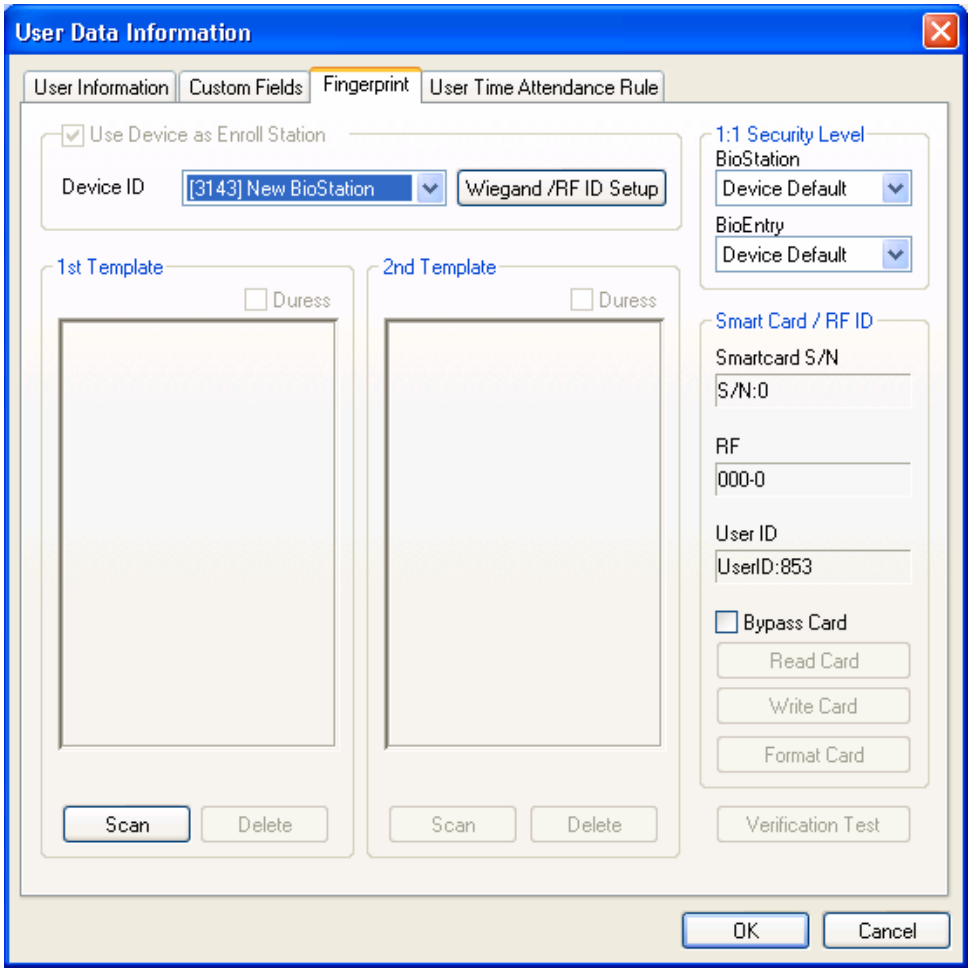
- In addition to the basic user information, you can add **Custom Fields** to the user information. If you do not need these **custom fields**, just skip the custom fields setting. To set up the custom fields, press Custom Fields tab.



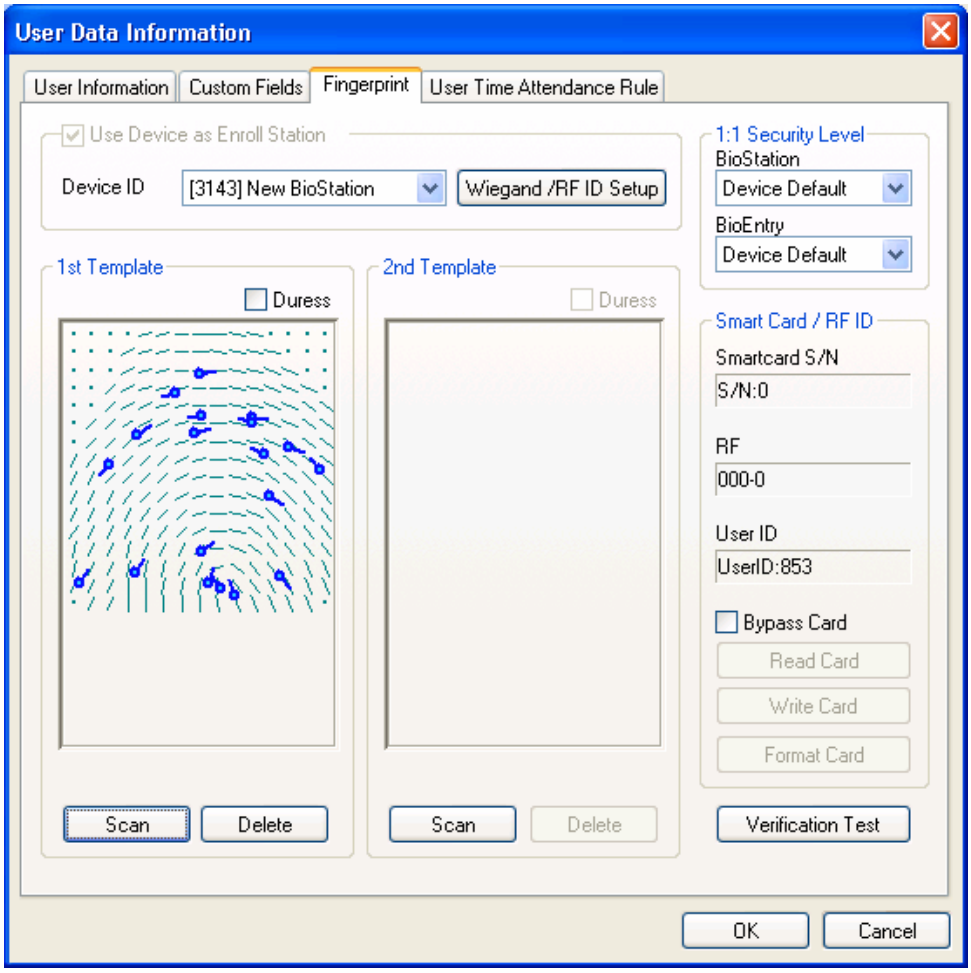
- Click the **Customize**... button.
- Check on the required Fields and enter the user information for those selected fields.



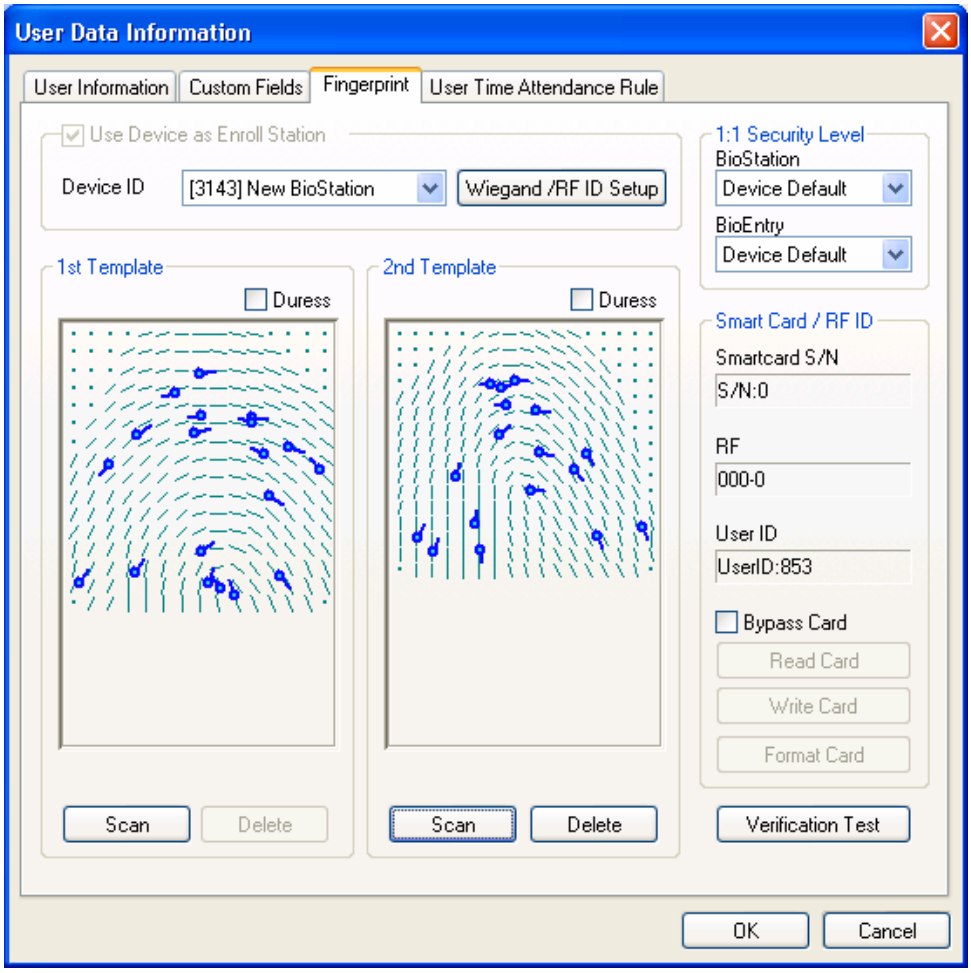
- After entering the user information, press the **OK** button.
- After filling out the custom fields, the following pop-up window will appear. On this window, you can see the details of your selected custom fields. Press **OK** button to save these custom fields.
- After entering the user information,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



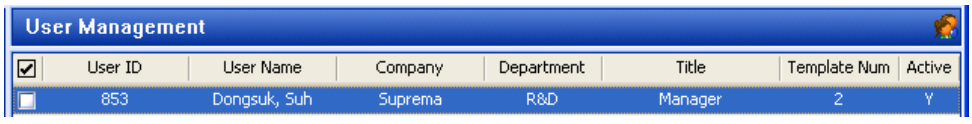
- Acquire first template by pressing the **Scan** button followed by touching finger on the USB fingerprint scanner twice.



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

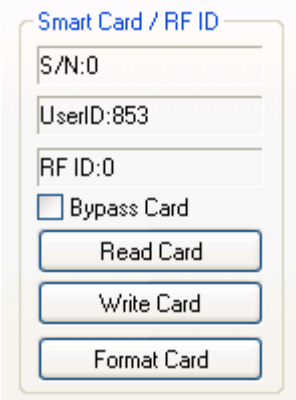


- Press the **OK** button to complete the registration process. Then, you can see the information of the registered user on the user list window. It means that user's information is added to the database on host PC.

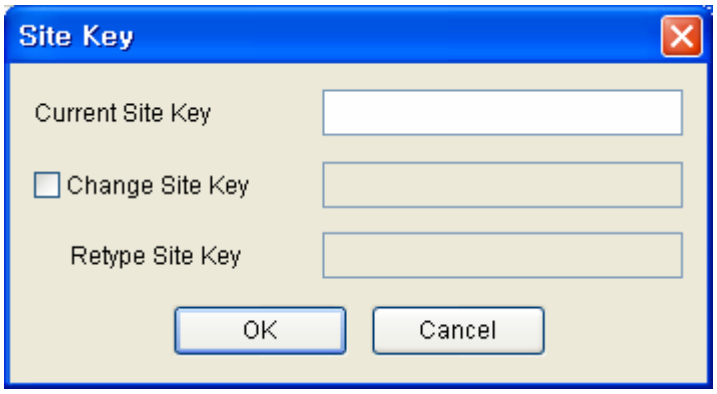


2.2.3. Step 3: Issuing user smart card

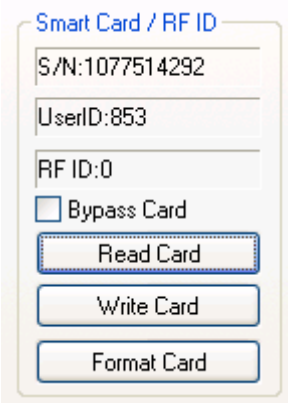
- Double click the registered user on the user list. Then, the user information window appears showing the registered information of the user.
- Click **Fingerprint** tab on user information window.
- Place a smart card on PC USB smart card device and press **Write** button.



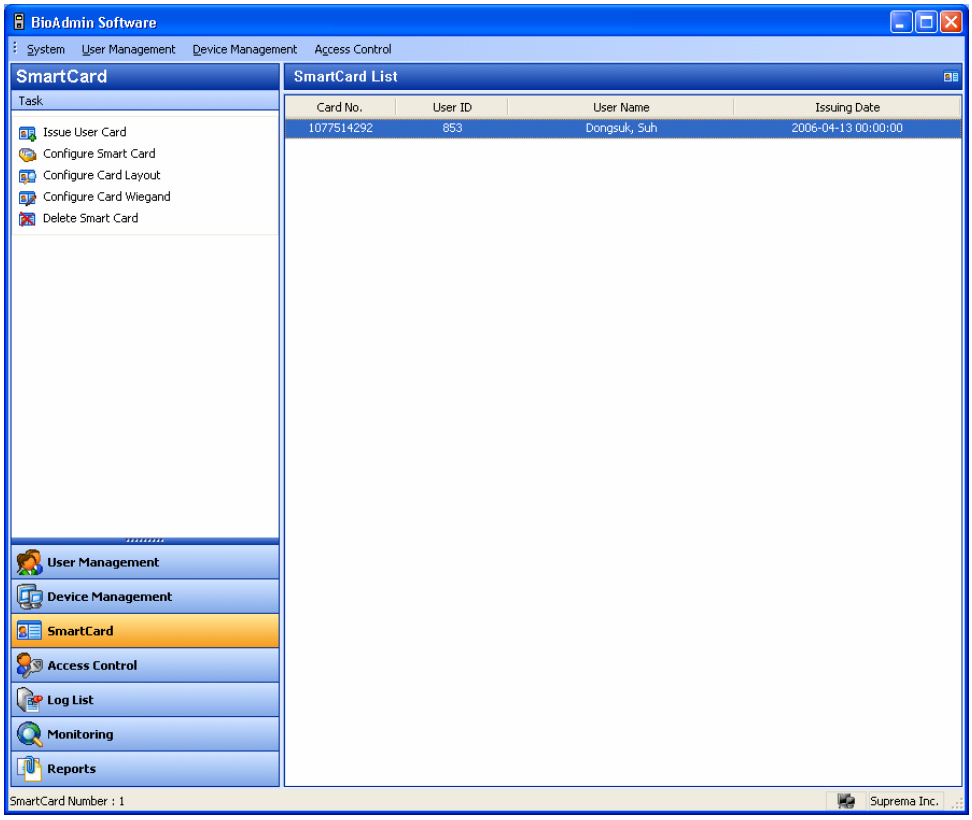
- At first trial, site key management window appears. If the key input remains blank, factory default key is used. So, just press **OK** button to complete issuing process if the site key was not changed from factory setting.



- 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.



2.2.4. Step 4: Enroll user ID in 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.

2.2.5. Step 5: Authentication Test

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

- First, place the user's smart card in front of the device below the sensor. Then, amber LED blinks rapidly indicating that the device 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.

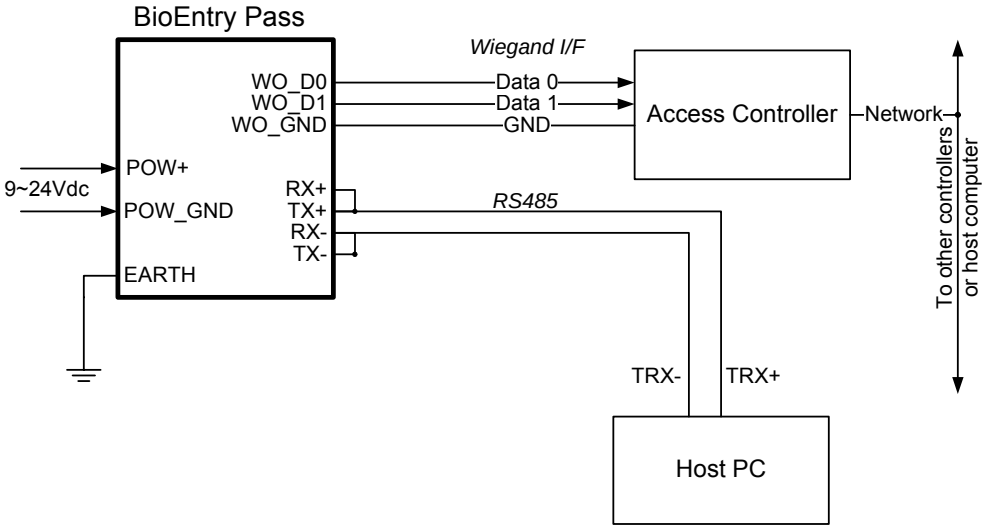
- On successful verification, the Wiegand string is also sent to the controller, which can be checked by operation of relay on the controller.

2.3. Quick start with BioEntry Pass

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

2.3.1. Step 1: Hardware installation

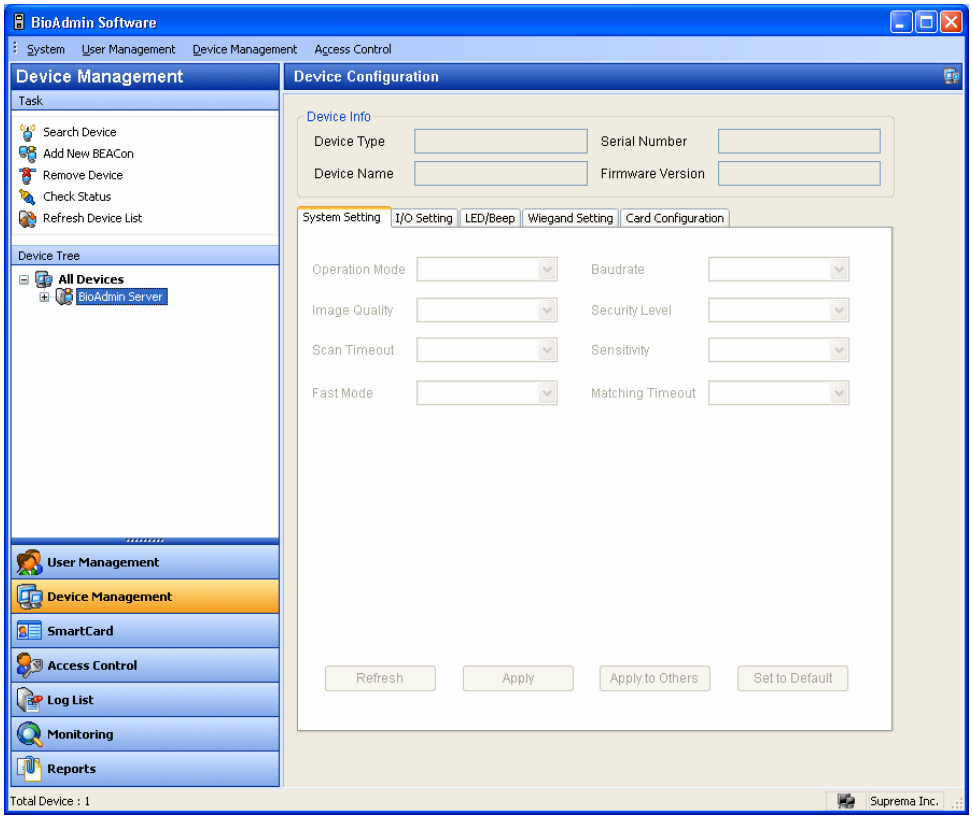
In this configuration, the device is connected to an external controller via Wiegand interface as well as to the host PC through RS485 interface. It is assumed that the controller supports the standard 26 bit Wiegand format as default of BioEntry device.



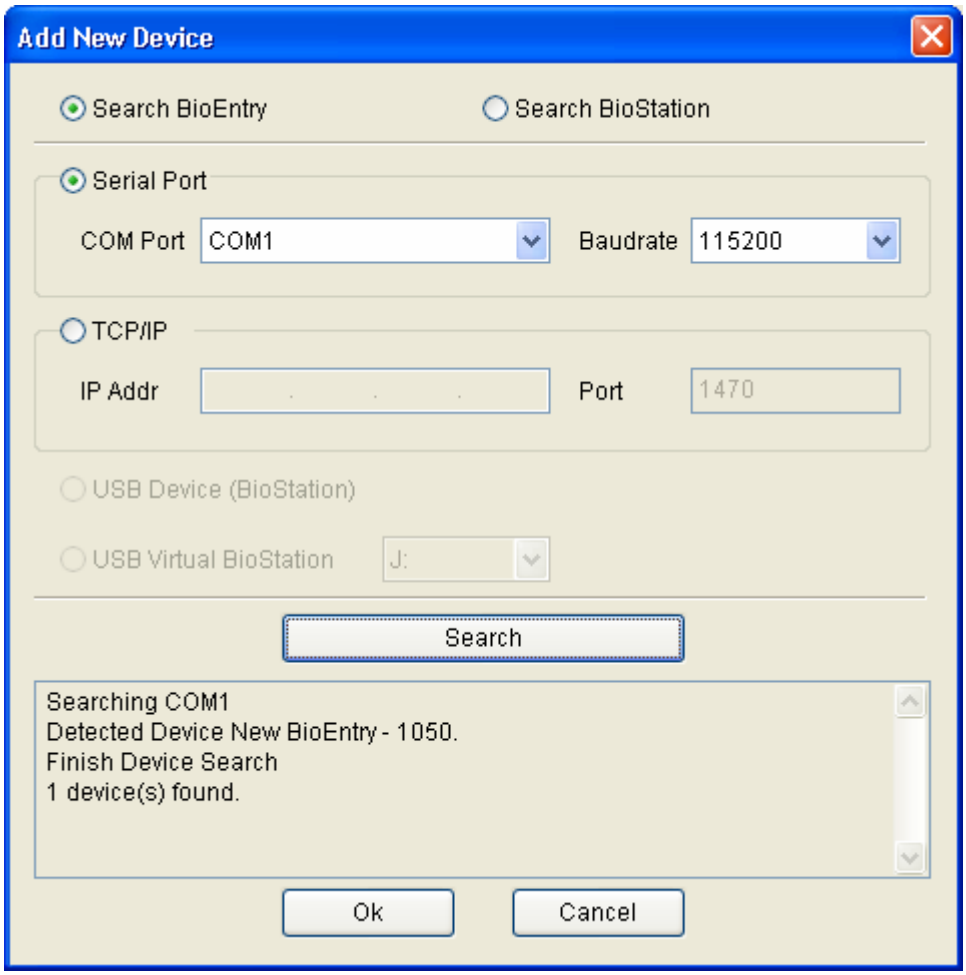
For more details on the installation, refer to the BioEntry Installation manual or BEACon Operation Manual.

2.3.2. Step 2: Search new device

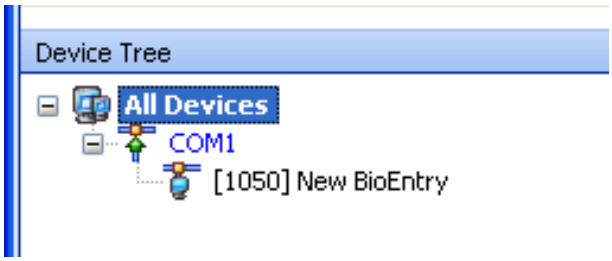
- Run BioAdmin software.
- Enter Login ID and password. By factory default, the initial Login ID is "**admin**" and the password is blank
- Select **Device Management** on the Main menu, then device management page will appear on the main window.



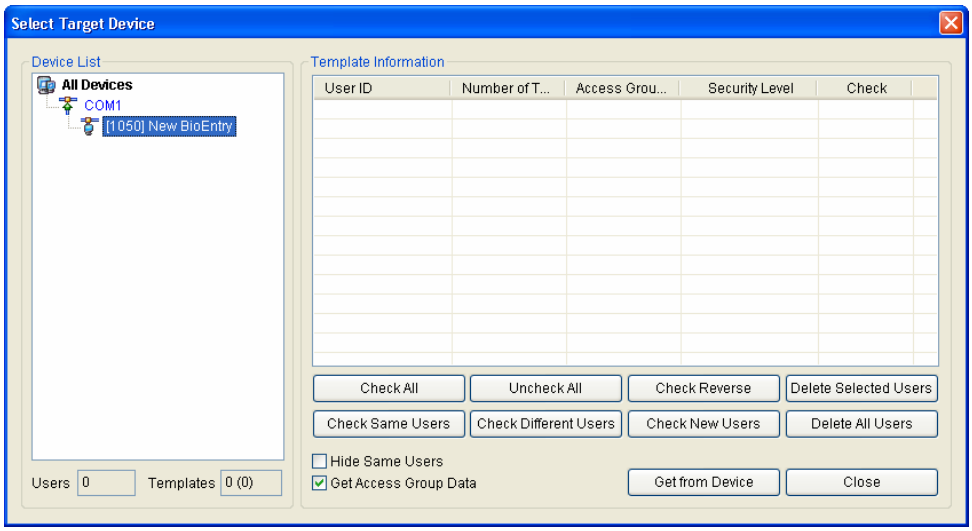
- Select **Search** Device menu, click **Search BioEntry**, select either serial port or TCP/PI and then press search button. If device is found as a result of search, result report reading '--- device(s) found' is shown. Press **OK** button to select device.



- If the devices are connected properly, new device ID appears on the Device Tree window.

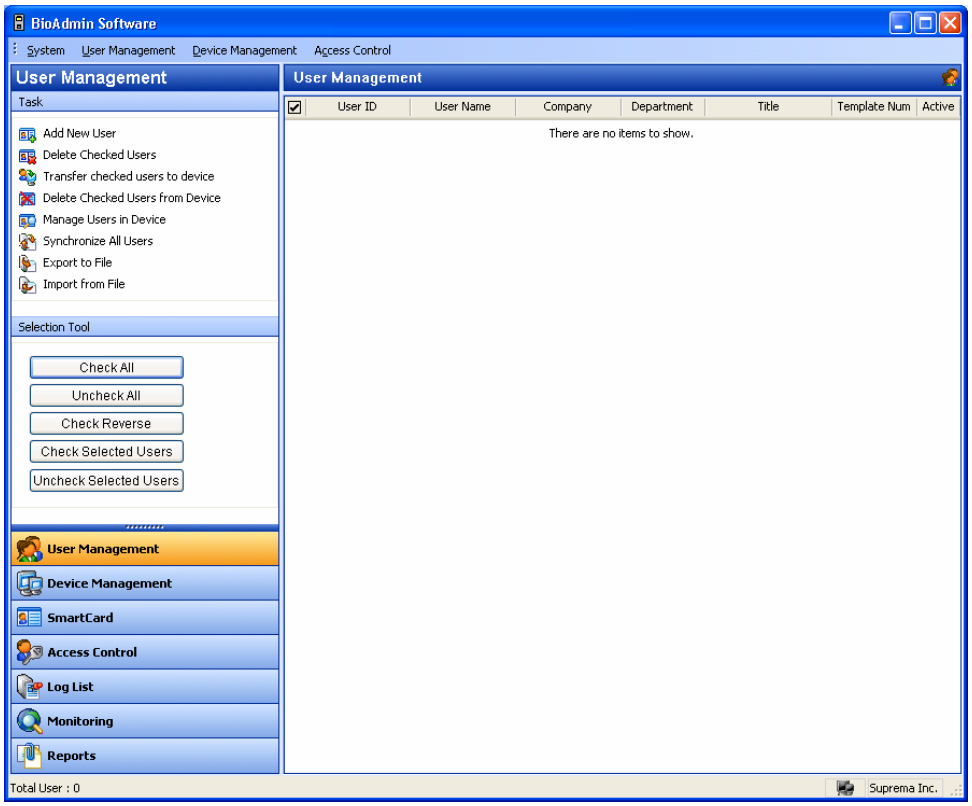


- Select **User Management** button on main menu and select **Manage users in device** on task window.
- Once device is selected, fingerprint information such as user ID, number of fingerprint, access group, security level and Check (to select) is displayed.

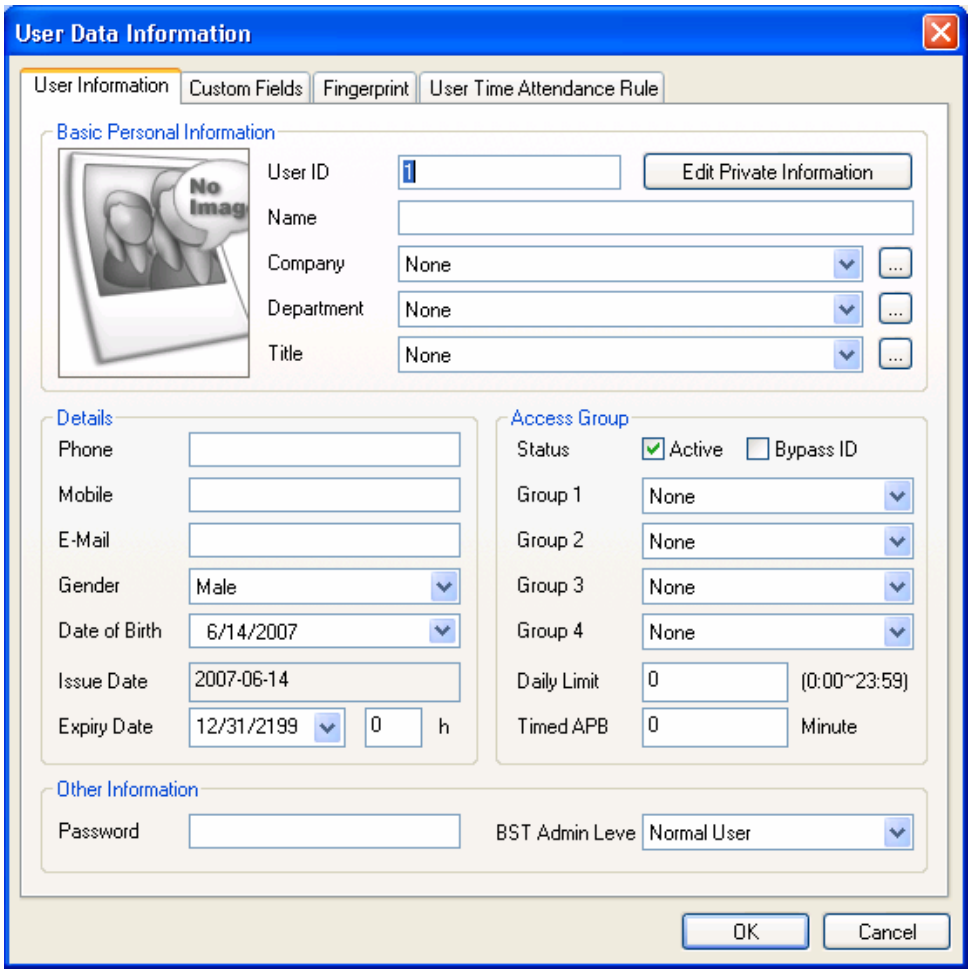


2.3.3. Step 3: Enroll user

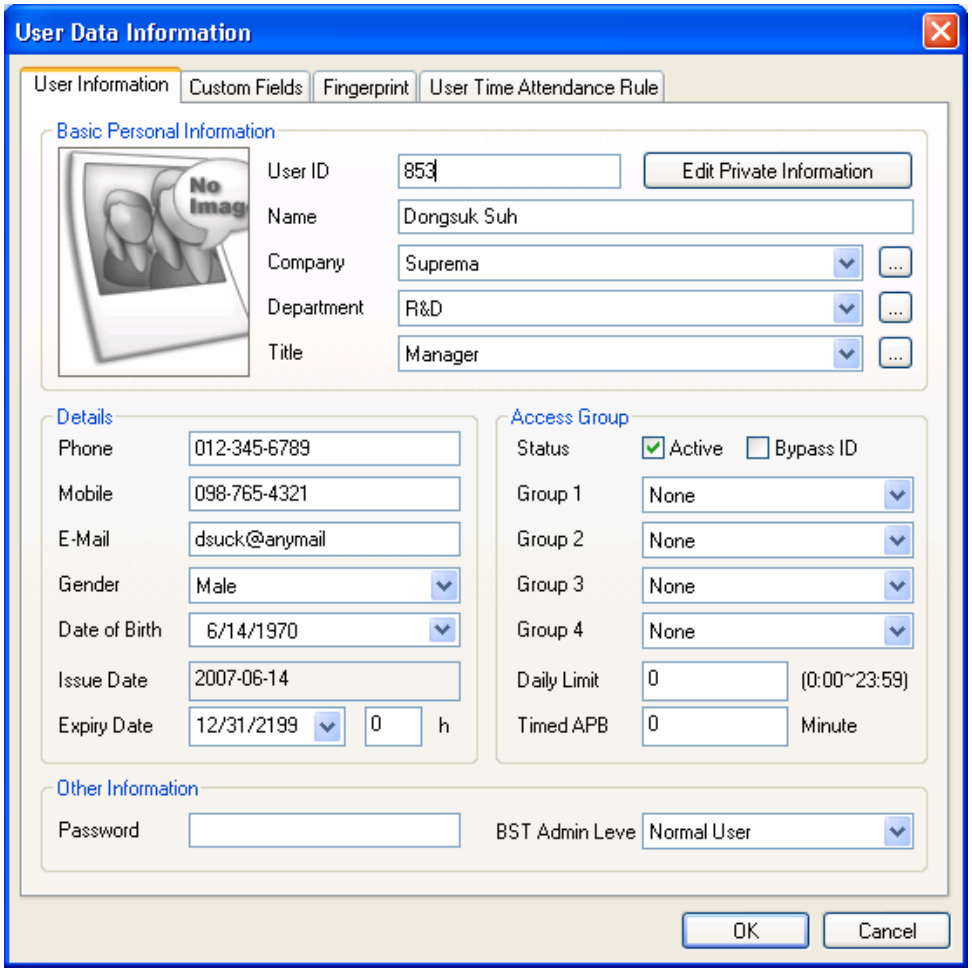
- Select the **User Management** menu, then the user management page appears on the main window



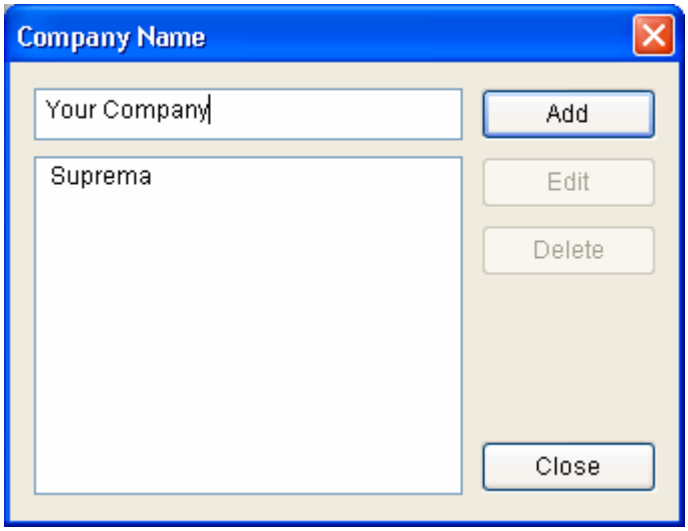
- Select the **Add New User** menu on the task window, and then the pop-up window appears.



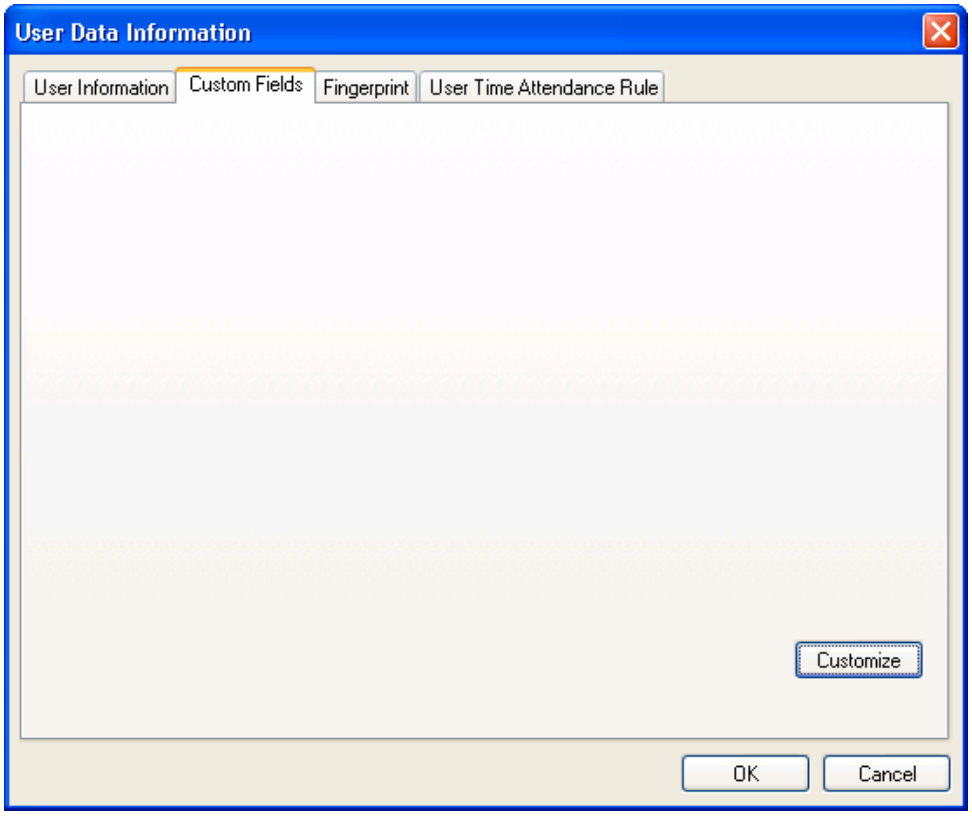
- Enter the user information on the **User Information** tab.



- 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.

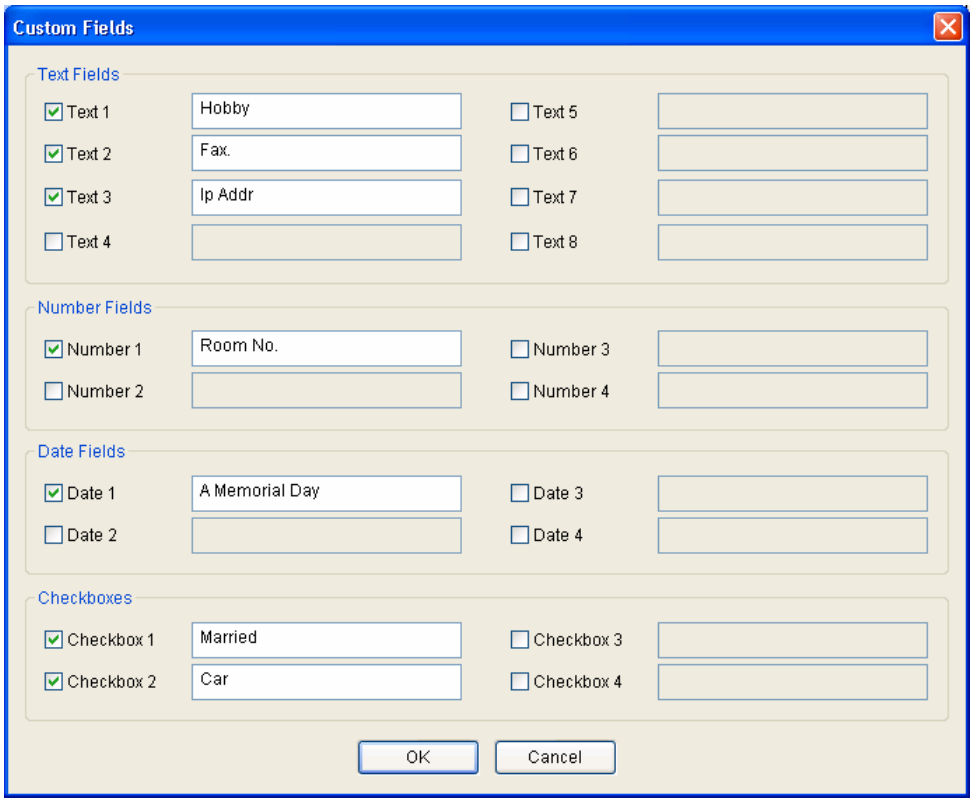


- In addition to the basic user information, you can add the **Custom Fields** to the user information. If you do not need these custom fields, just skip the custom fields setting. To set up the custom fields, press the **Custom Fields** tab.

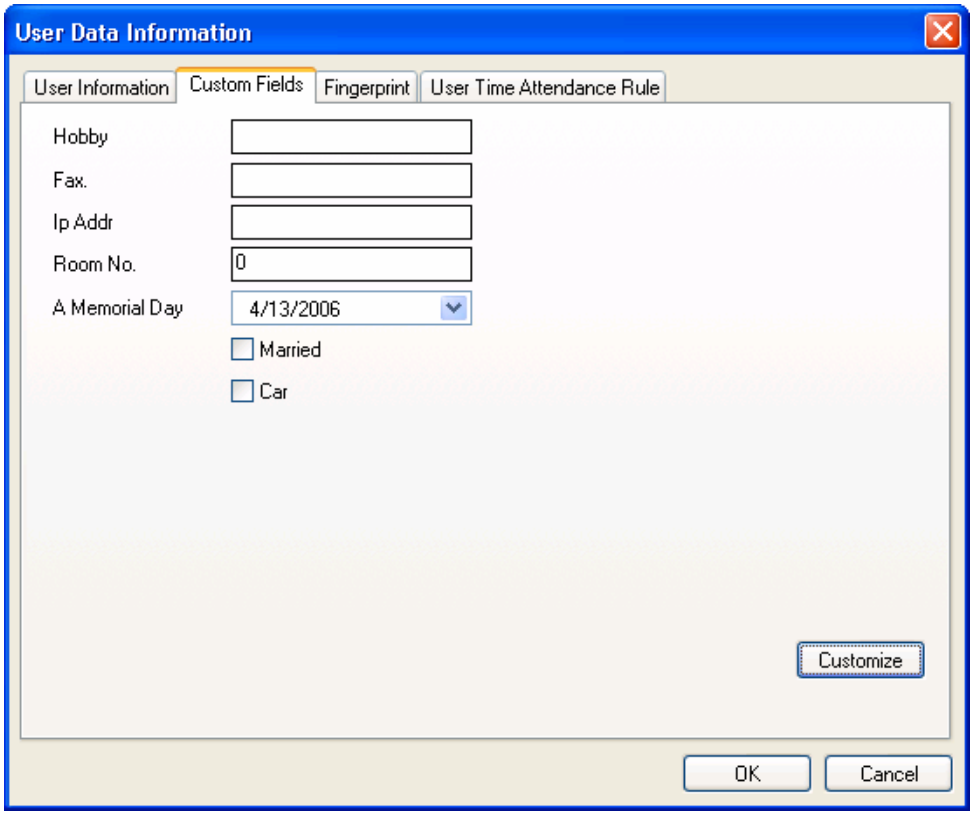


- Click the **Customize**... button.

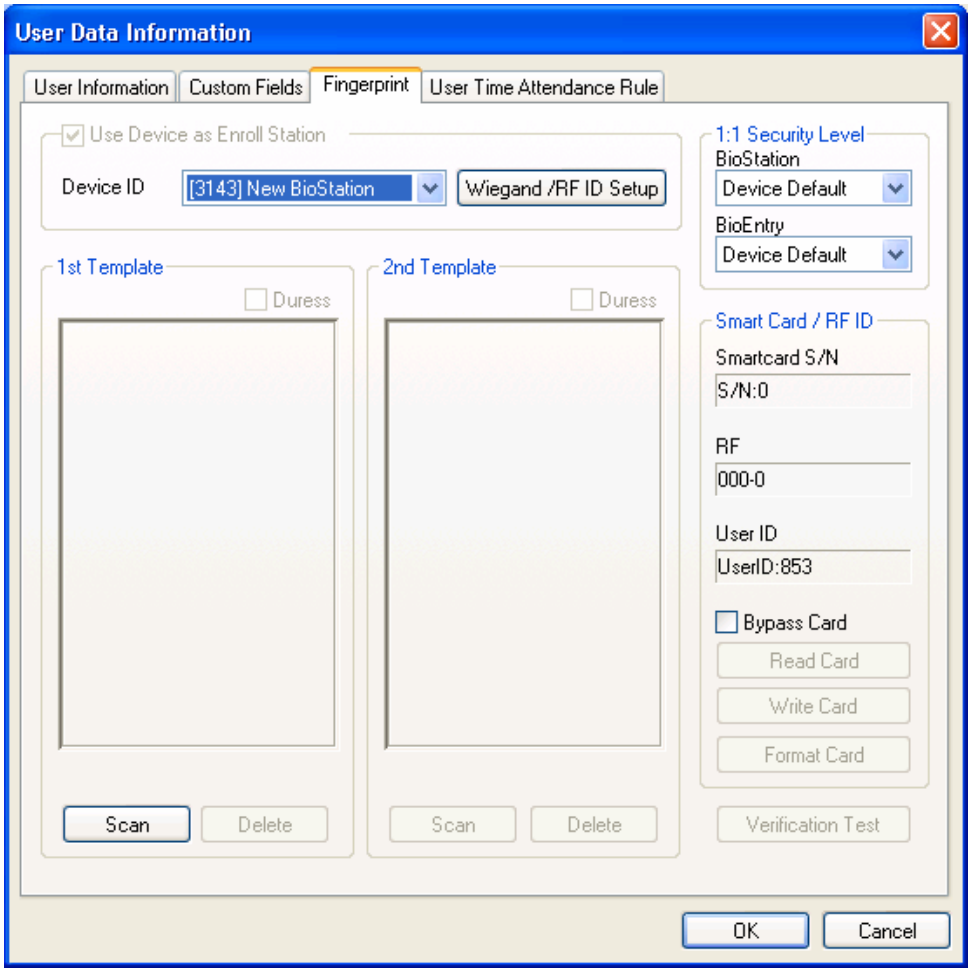
- Check on the required fields and enter the user information for those selected fields.
- After entering the user information, press the **OK** button.



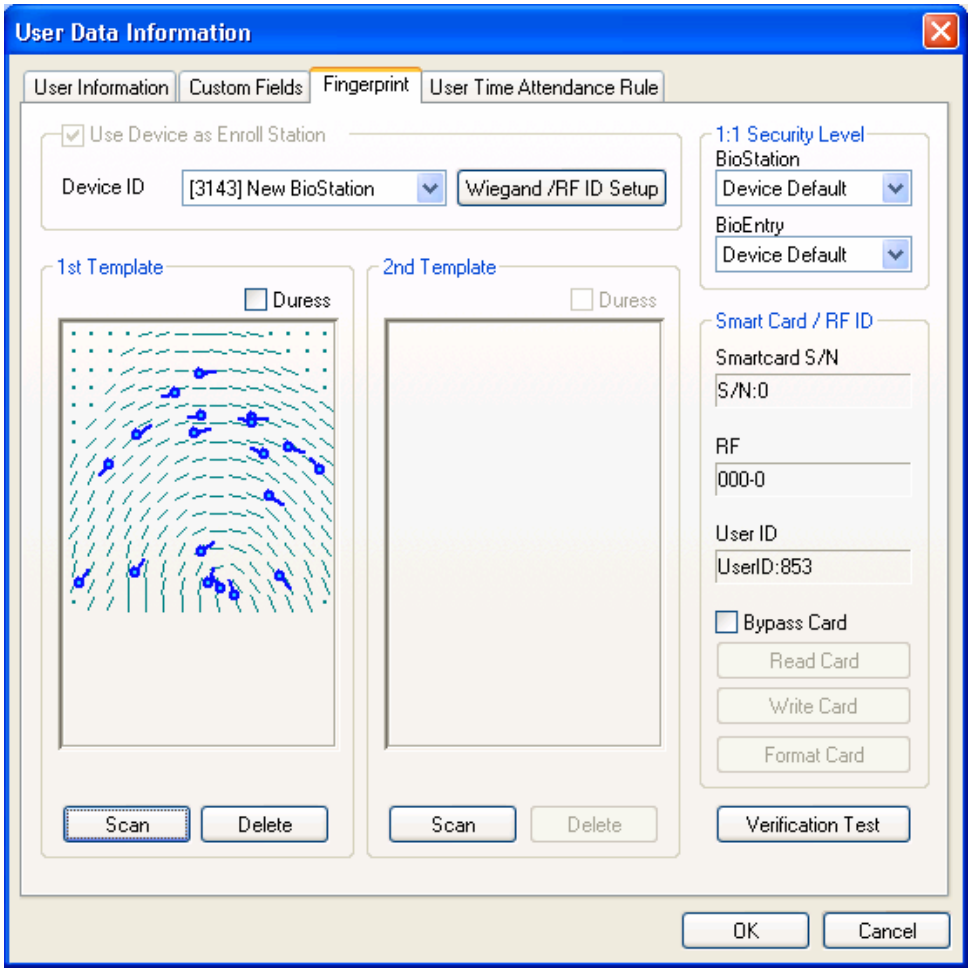
- After filling out the custom fields, following the pop-up window will appear. On this window, you can see the detail of your selected custom fields. Press the **OK** button to save these custom fields.



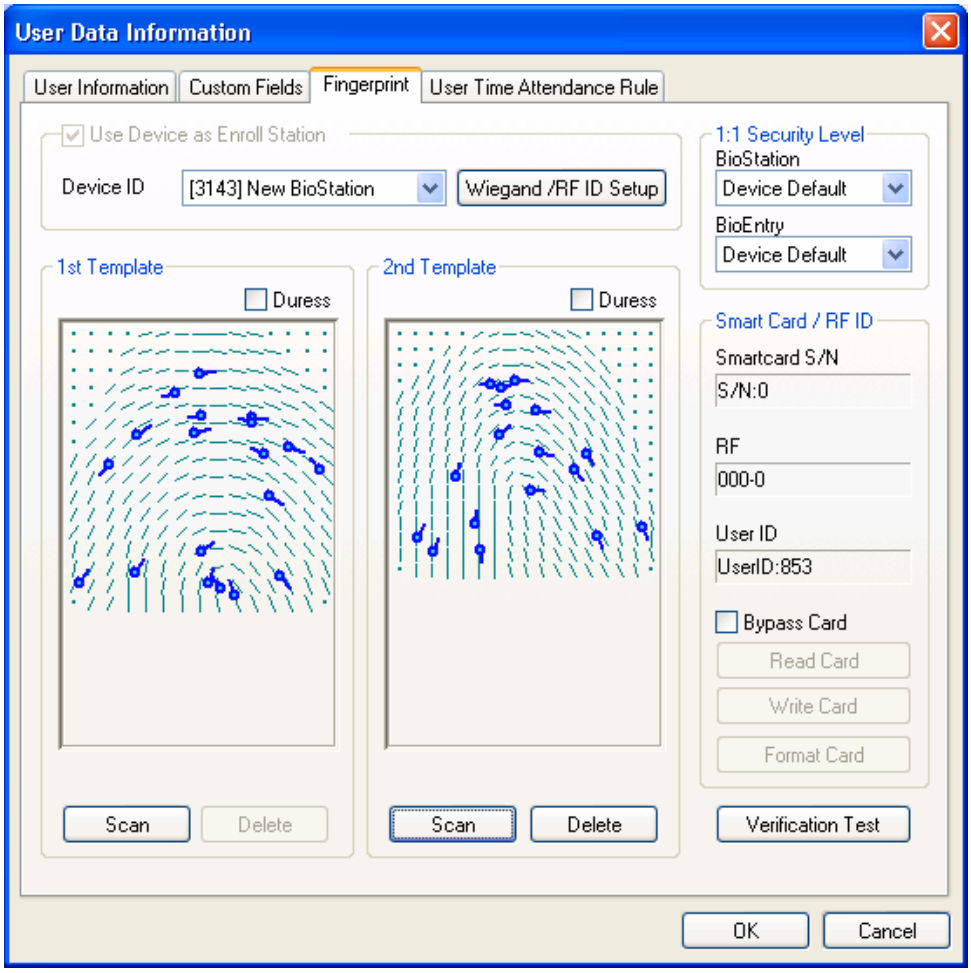
- After entering the user information, press the **Fingerprint** tab to enroll user's fingerprint templates.



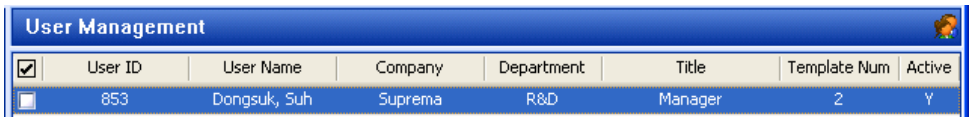
- Acquire first template by pressing the **Scan** button followed by touching a finger on the USB fingerprint scanner twice.



- 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.

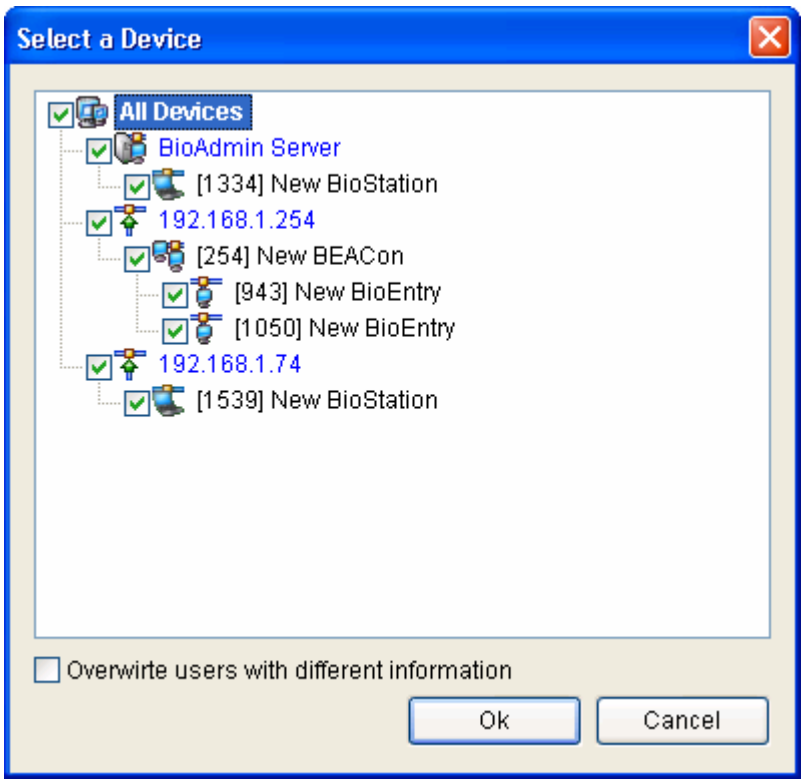


2.3.4. Step 4: Enroll user with 'transfer checked user to device' menu.

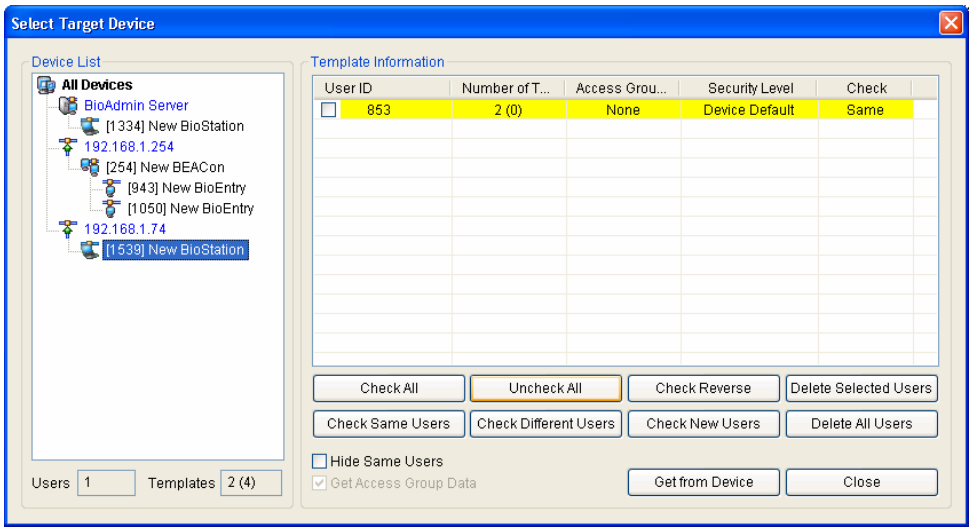
Transfer to Device is used to transfer the user database of the host PC to BioEntry™ devices. The user information such as User ID, templates, access group, and security level is transferred by this process.

- Check the registered user to transfer

- Select the Transfer Checked Users to Device button and select the devices to transfer the user data.



- Select the **Manage Users in Device** button to see the user list enrolled in the selected device. If the color of user data is yellow, it means the user data has been successfully transferred to the device.



2.3.5. Step 5: Enroll user ID in 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.

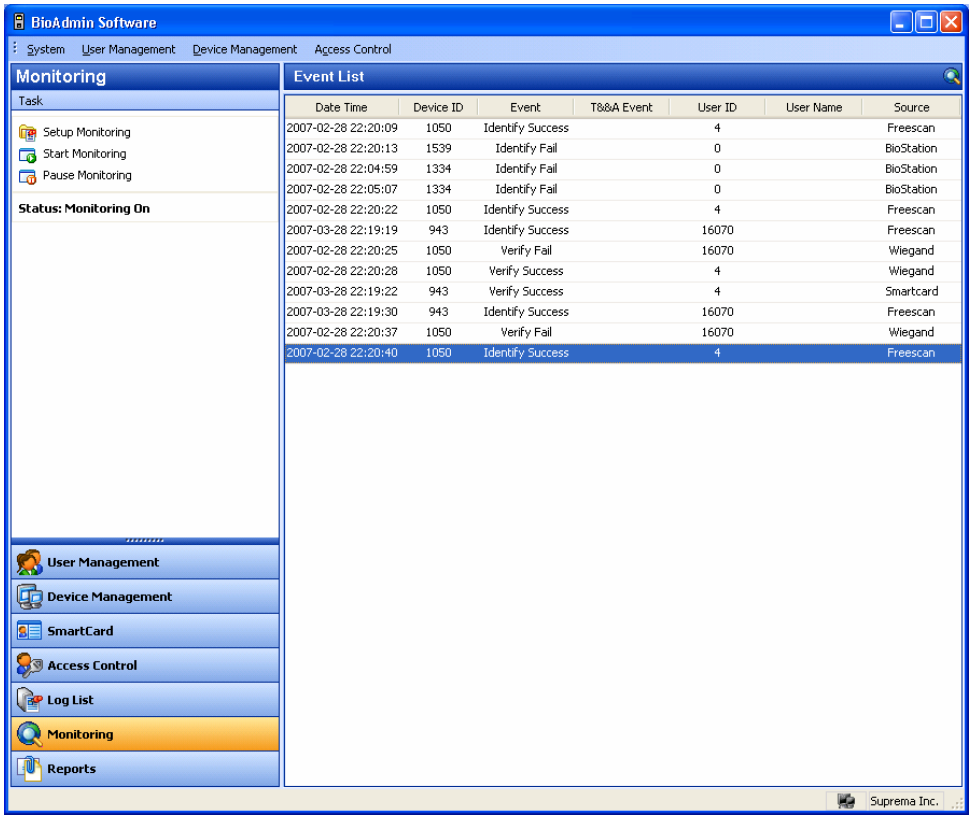
If you are using Suprema's BEACon controller, you can just skip this additional registration to the controller.

2.3.6. Step 6: Authentication test

- Amber LED on the device blinks slowly indicating that the device 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.

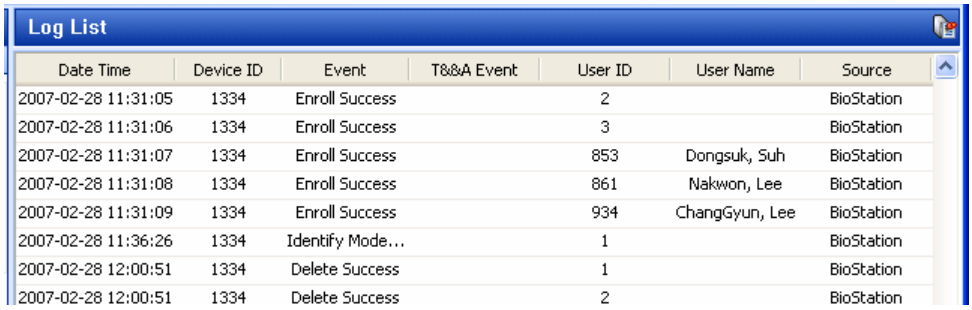
2.3.7. Step 7: Monitoring

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



2.3.8. Step 8 : Check log

- Select the **Reports** menu. Then, the report list window appears on the main window.
- Select the **Get Recent Logs / Auto Upload** button to see the updated event log data added to the existing log list of BioAdmin.



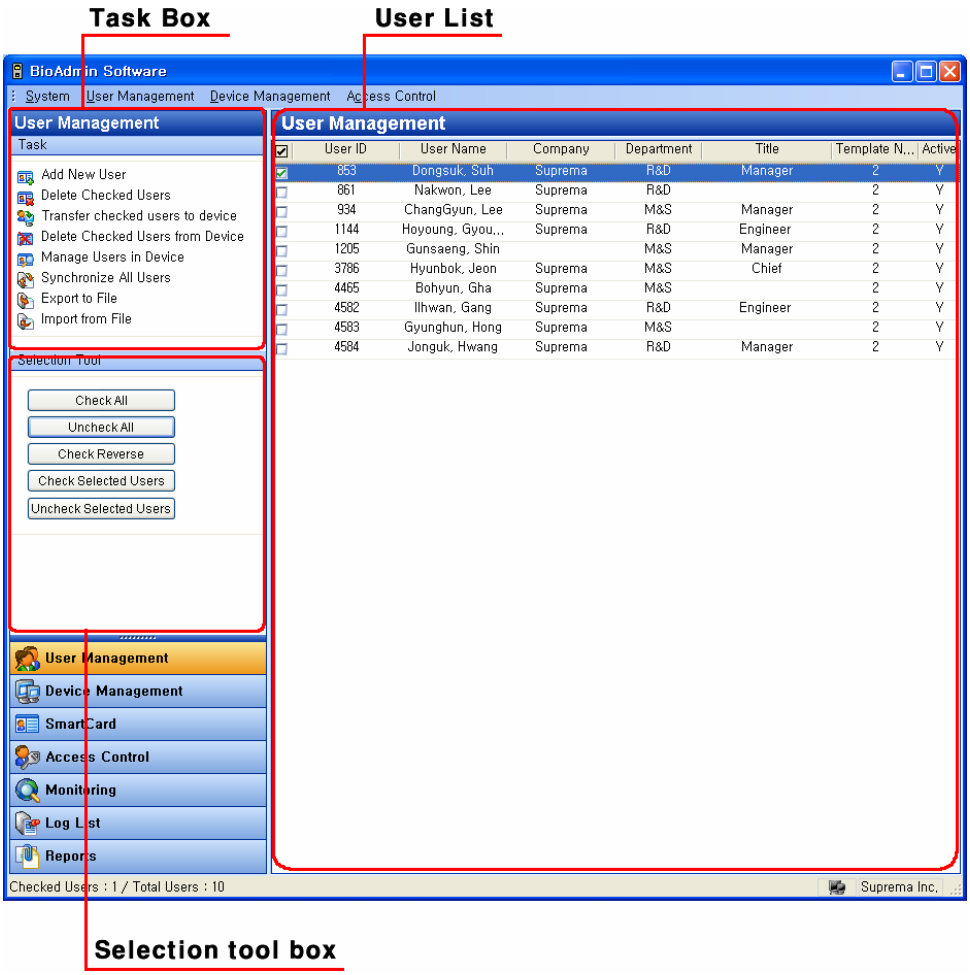
3. User Management

User management covers the following operations:

- Add new user
- Delete checked user
- Transfer checked user to device
- Delete checked user from device
- Manage users in device
- Synchronize all users
- Export to file
- Upload from file

3.1. Configuration 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.

3.2. User List window

User list includes the following information on the users.

- Shows basic information such as user ID, name, company, dept., position title, number of enrolled fingerprint and status.
- Double click user ID to pop up user information window. User information has 4 tabs, i.e. User information, custom field, fingerprint, and user time attendance rule.
- Fingerprint templates (fingerprint image is never stored)

> Note : What is activation in access group setting? It is used when transferring user data in host PC to device. If activation is not on (checked) upon transferring checked in user list to device, user data can't be transferred and data in device is deleted.
>
> For instance, when one returns to work after having been excluded from access group and inactive due to dispatch or long term leave, activate him/her and manage user list.

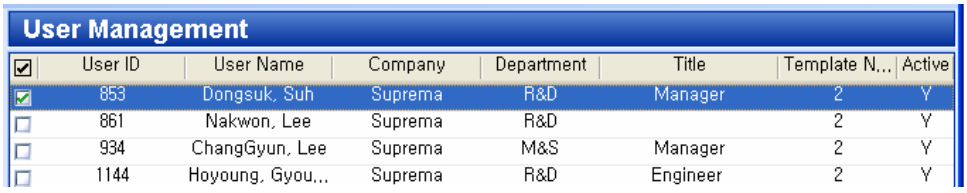
3.3. User List Display Setting

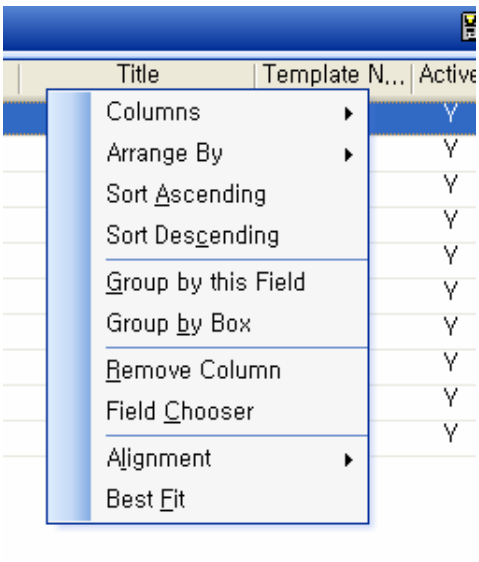
You can customize the display of the user list.

Detailed operations are as follows.

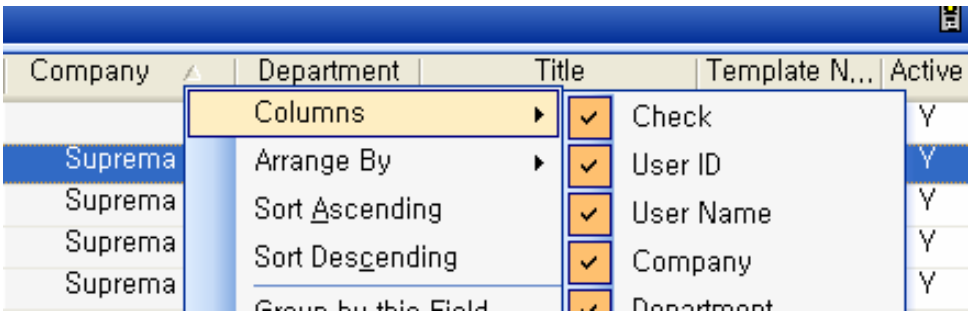
- Press the right button of your mouse on the column header of User List.

> Note : What is "Column Header"? It is on the head of row (user ID, name, company, dept.) on user list window.

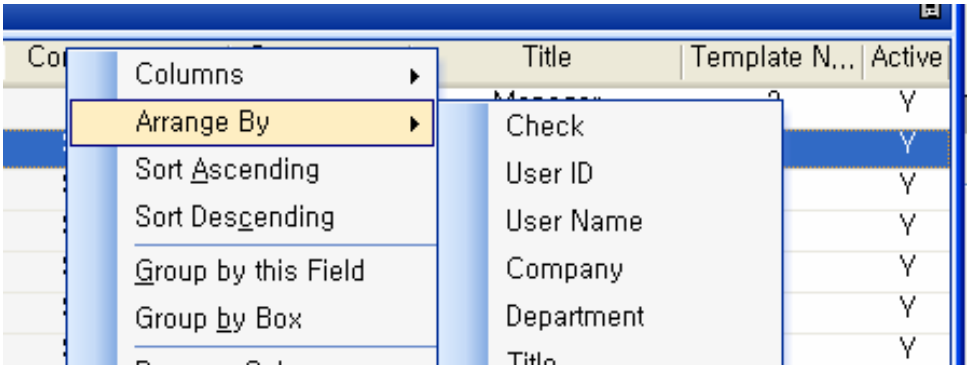




- Press the **Columns** button and check on your required columns to show them on the user list.

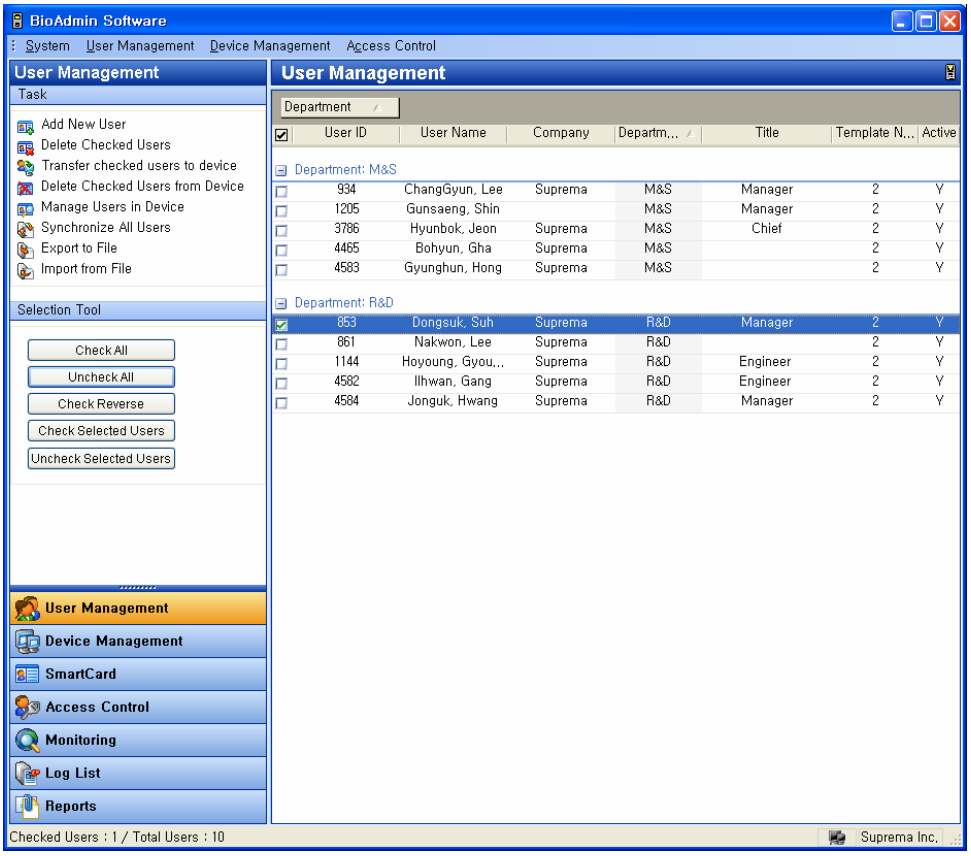


- Press the **Arrange By** button and select your required columns to array the user list by your selected column.

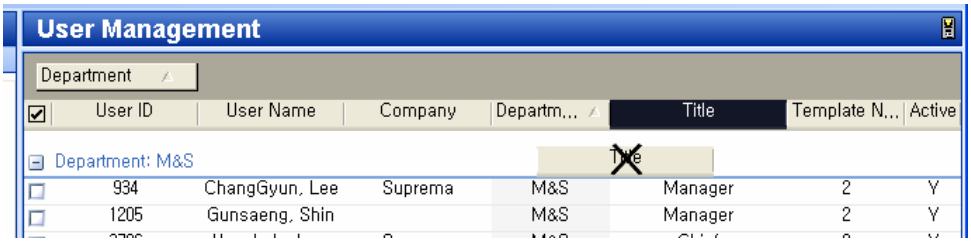


- Press the **Sort Ascending** button to array the user list in ascending order.
- Press the **Sort Descending** button to array the user list in descending order.

- 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.



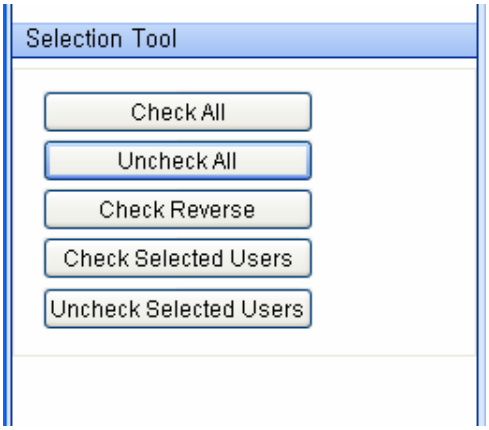
- Press the **Remove Column** button to remove a column from the header. Also, you can remove a column simply by dragging down the column from the column header.



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

3.4. Select user

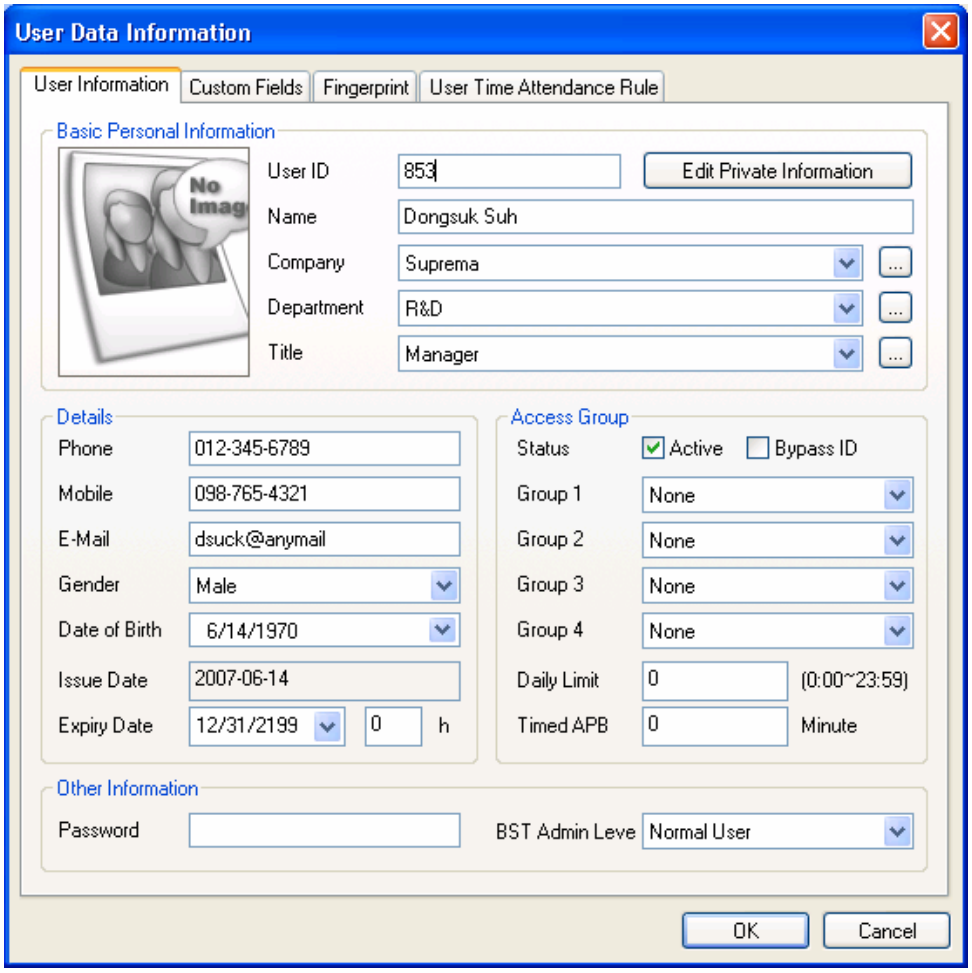
Users can be chosen for selective processing of operations, such as transfer, removal, or exportation. You can select the required user simply by using the check box on the user list,



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

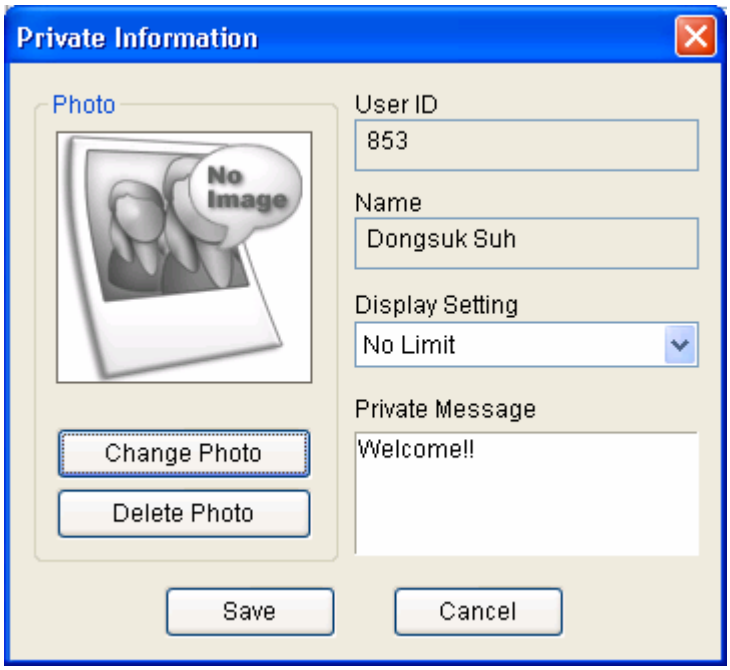
3.5. Add New User

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



3.5.1. User information

- In user information, you can enter basic personal information, details information, access group, other information, and additional information for BioStation. In basic personal information, enter user ID, name, company, dept. and title. For details, enter telephone number, mobile phone number, email, gender, and date of birth. Make sure to check 'Active' in access group. Otherwise, database in device will be deleted.
- Edit Private Information



- Change photo and message when succeeded in verification, and configure display condition, which should be used 'Private Information' of the device.

- Access Group
  - Enter the access group information for each user.
  - To apply the designated access group information to each user, please check on the **Active** option and sent transmit this user to the BioStation and BioEntry. If you do not check on this option or do not transmit the user to the BioStation or BioEntry, access group will not be applied to each user.
  - If you check on **Bypass ID** option, that user will be able to access the door just by placing this card to the BioStation without fingerprint or password.
  - **Auth Limit** means the number of access that the user is allowed in a day (from 00:00 to 24:00 of the day). If you do not want to restrict the number of access for a user, leave this menu as the default, 0.
  - **Timed** means the minimum time interval required for access of the same user. If you set this menu as 5, that user will not be able to enter the door again within 5 minutes.

- Other Information
  - The Password on this menu is required when the BioStation requires the user's password. Also, users should enter this password when they log in

to the BioAdmin Client to check their log information.

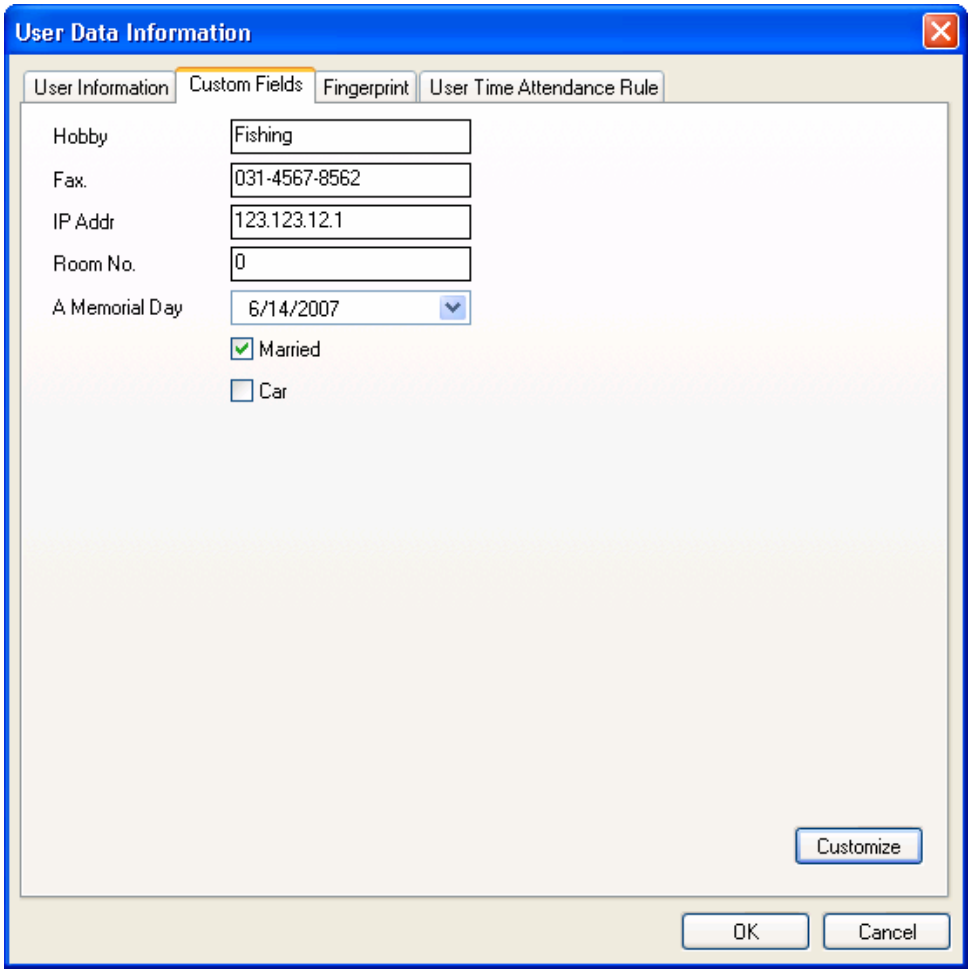
- BioStation admin level : On this menu, you can select the user as an administrator for BioStation terminal.

Note : in user information, user ID should be entered as it's a required field but the rest fields can be left blank.

3.5.2. Custom field

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

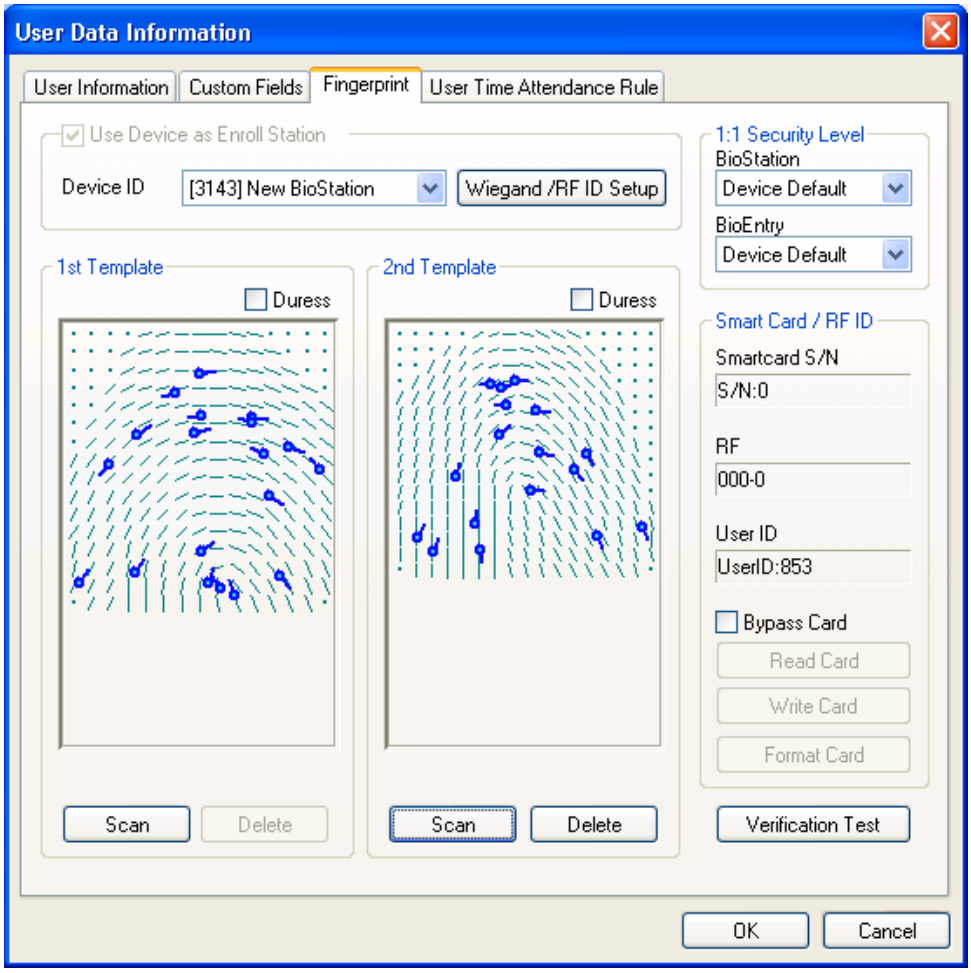
- Customize… button enables the pop-up window to add the customized user information column. After filling out the required contents, press the OK button.



Note : Custom fields may look like a blank page but if you click settings on the right lower end, a display where you are to set custom fields such as string, number, date and checkbox appears. If you check such fields, items are generated in blank custom fields.

3.5.3. Fingerprint

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 device 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 device ID, BioEntry™ device 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 device. After a template is acquired, enable the **Duress** check box to indicate that the template should be saved as duress mode.

> Note : What is duress mode?
>
> Duress finger can be used in a situation when one is threatened by a thief in front of a door. If duress finger is entered, door is opened normally but it can be set to sound an emergency alarm or ring an emergency call which has been set as output port. For instance, in case of enrolling 2 fingers, the first finger can be enrolled as normal finger whereas the second finger as duress finger. Duress finger should be a different finger from a normal finger enrolled beforehand.

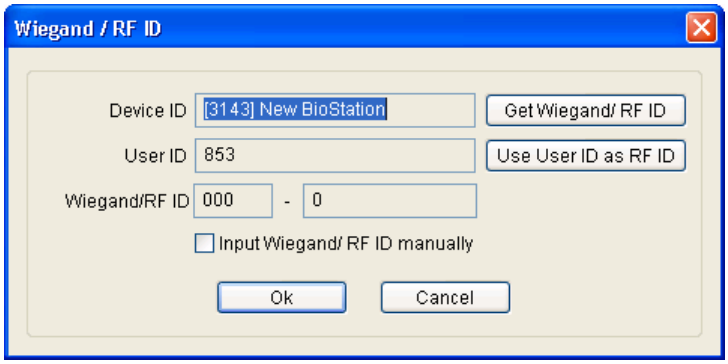
- Delete fingerprint

  To delete fingerprint, delete from the second fingerprint information on the right. The first fingerprint information can be deleted after the second fingerprint information is deleted.

- 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 device. Then, a message will appear to show the matching result.

- Wiegand / RF ID Set up



If you use BioStation RF or use the normal BioStation along with an external Wiegnad card reader, you need to allocate the card ID to each user. Press this button to designate the users' card ID.

- **Get Wiegand / RF ID :** If you press **Get Wiegand / RF ID** button, BioStation RF (or external Wiegand card reader) will be waiting for the card. If the user put his card to the BioStation (or to the external Wiegand card reader), the Wiegand ID of that card will be registered as the user's card ID. Therefore, you can use this option to get the Wiegand ID from the card and apply it to the user.
- **Use User ID as RF ID :** If you press **Use User ID as RF ID** button, Wiegand card ID is entered as same as the user ID. This menu is useful when the users were already using Wiegand cards of which card ID was set as same as the user ID.
- **Input Wiegand / RF ID manually :** If you press **Input Wiegand / RF ID manually** button, you can enter the Wiegand / RF ID manually.

- 1:1 Security Level.

  You can change the security level for the 1:1 verification of BioEntry and BioStation. If a user's fingerprint condition is very poor and he often fails in 1:1 verification, administrator may enroll his fingerprint after lowering the 1:1 security level for that user.

3.5.4. Issue user 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 device
- 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 device ID. Otherwise, PC USB device is used as a card issuer.

3.5.5. Issue with PC USB smart card device

- Place the target smart card on the PC smart card device

- 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 device.

3.5.6. Issue with BioEntry Smart

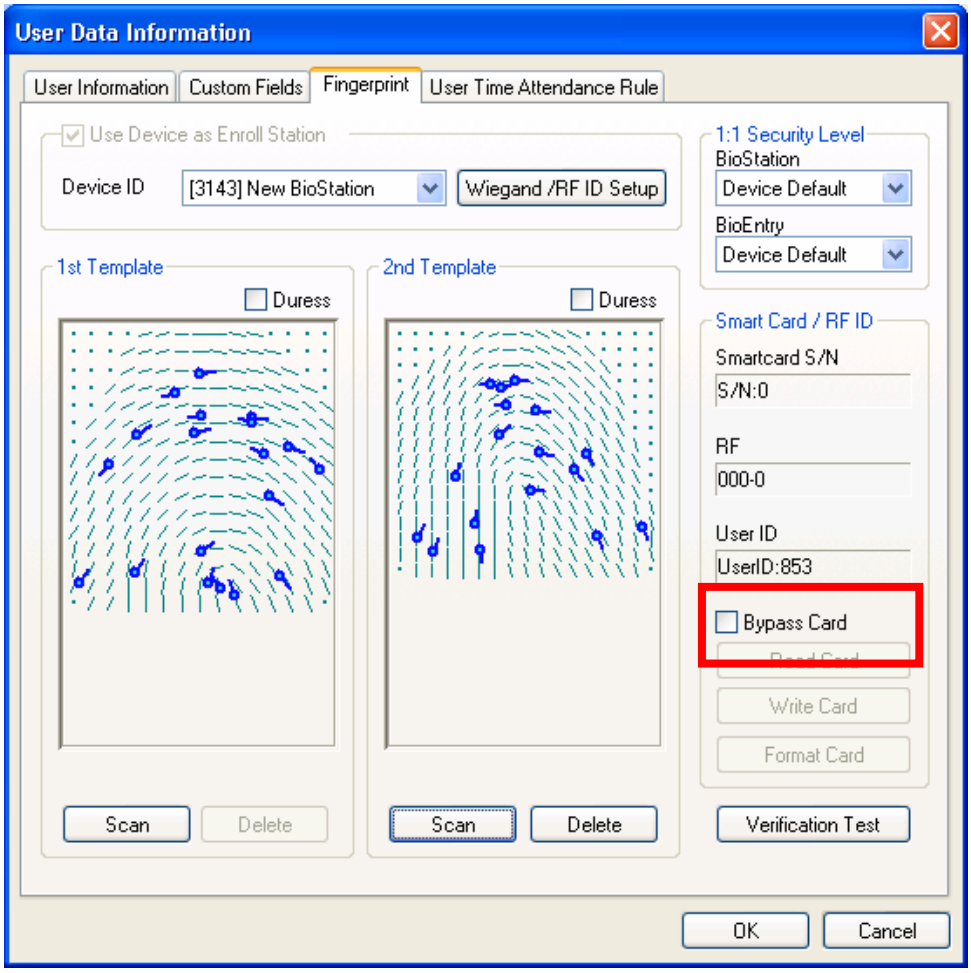
- Place the target smart card at selected BioEntry Smart
- Press the **Write** button to initiate issuing. Since the site key management information is stored on BioEntry, issuing is processed without requesting site key.

3.5.7. User security level and all-time pass card (Bypass) setting

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 **Device Default** is selected, security level configured on BioEntry Smart device is used.

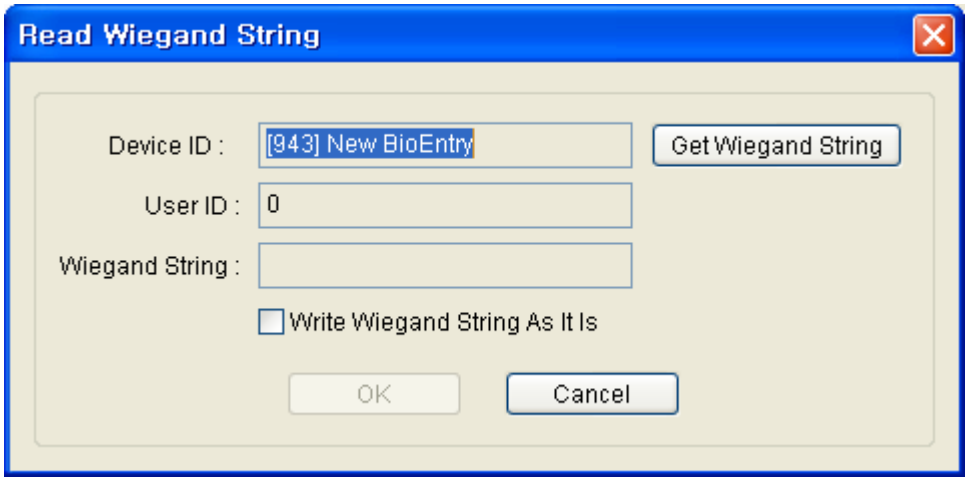
To issue all-time pass card (bypass card), you can choose bypass card option.

Note : What is bypass card? Device authorizes a user with a card without fingerprint authentication process.



3.5.8. Wiegand string setting 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 device should be connected to the Wiegand input port of the selected BioEntry device.



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 device.
- The Wiegand string received from the device 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.

3.5.9. Read 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 device 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.

3.5.10. Card format

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.

3.5.11. Notes on card issue

- 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.

  Note : 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.

3.5.12. Rules on user T&A event control

This menu is used to set user time attendance rule. For the detailed operation, refer to Chapter 12 Report.

3.6. Delete checked user

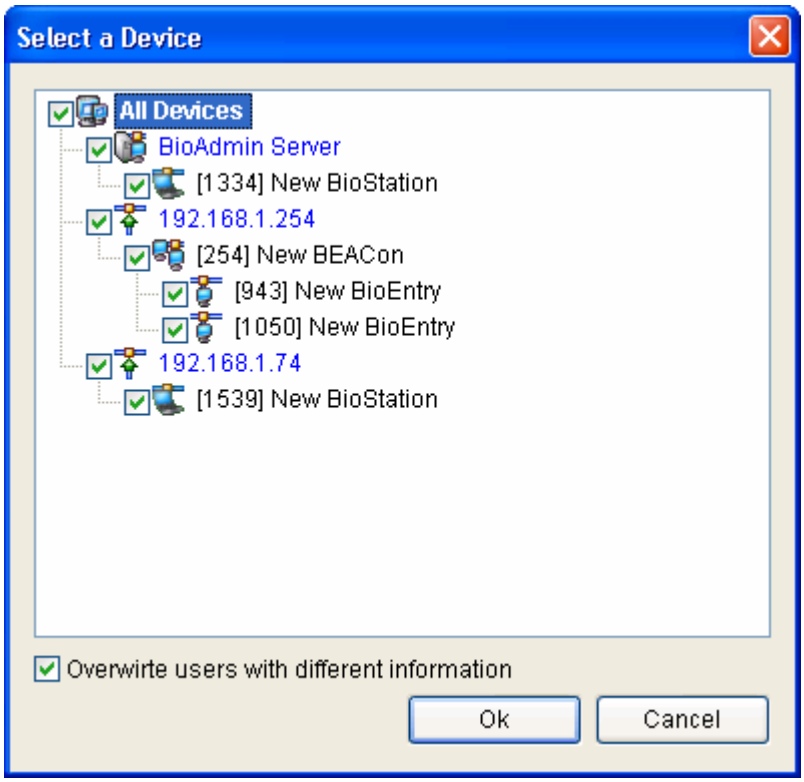
3.6.1. Delete checked user from BioAdmin software

Delete checked user information on user list window. If you check a user and click **delete checked user** in task box, a message “do you want to delete checked (selected) user?” appears. If you press ok button, checked user is deleted from BioAdmin of the host PC.

3.6.2. Synchronization deleted user information with device

If you transfer remaining user information after deleting a specific user, you can also delete such deleted user information from device.

3.7. Transfer checked user to device



Transfer checked users to device is to transfer user DB in host PC to device. To run a device, user data including fingerprint information should be transferred to device after user enrollment.

User information such as user ID, finger scan information, access group and security level is transferred through this process. Transfer procedure is processed in selected device, selected group or all devices linked on network. In how to select (check) user, user information can be transferred selectively.

Detailed operating process is as follows.

- Check a user to transfer.
- Press **transfer checked users to device** button.
- Select a device on select device window.
- In case user ID is same but user information is different, if you check overwrite, data in host PC will overwrite the same user's information in device.
- If not able to find a selected user in device, new user data is transferred from host PC database to device.

3.8. Delete checked users from device

On user list window, enrolled user can be deleted by **delete checked user from device** button.

Detailed operating process is as follows.

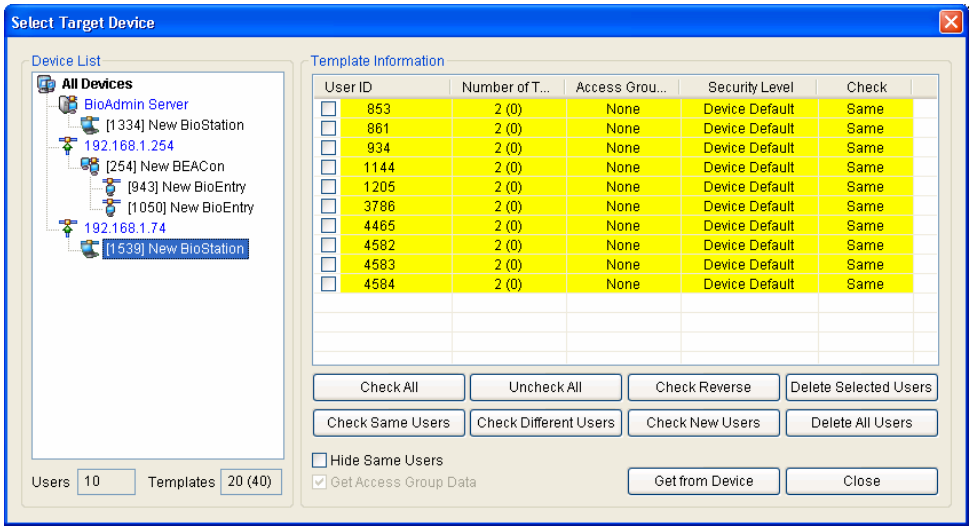
- Select a user to delete
- Press d**elete checked user from device** button on task window.
- Select a corresponding device on select device display.
- Selected (checked) user is not deleted on host PC user list. To delete it from host PC user list, press 'delete checked user' button.

> Note : Be careful in selecting a device in a network because it is a task to delete user information from selected device.

3.9. Manage users in device

Manage users in device is to upload user information from device to host PC database. User information such as user ID, fingerprint information, access group number, security level is uploaded thru this process.

In this menu, you can upload user database selectively from chosen device on network.



Detailed operating process is as follows.

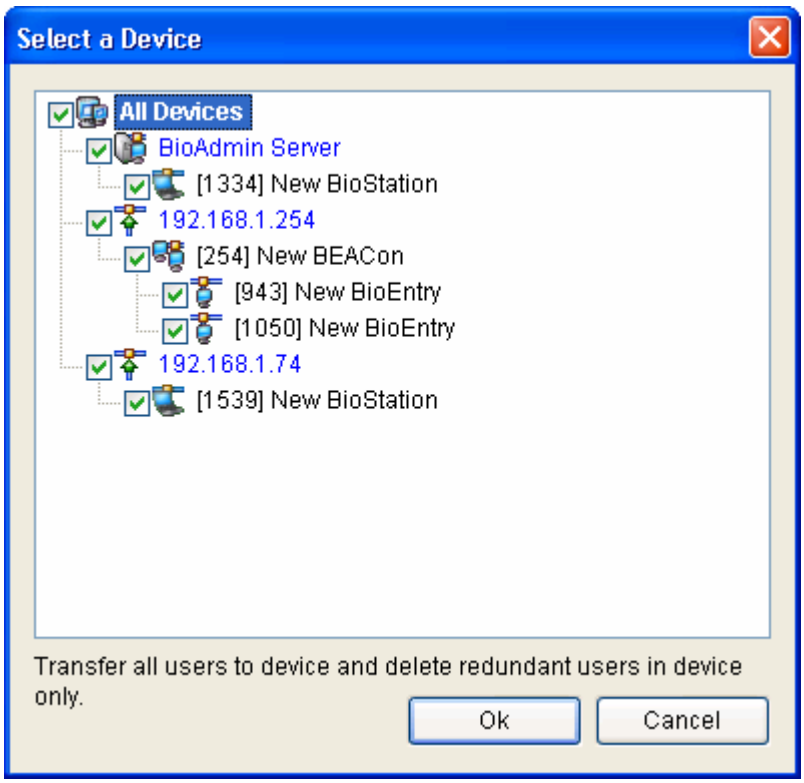
- Press **Manage users in device** button.
- Select a corresponding device on device list window.
- Under device list window, you can see user and number of fingerprint information enrolled in the selected device.
- User classification
  - Same user : user whose user information in BioAdmin software corresponds to user information uploaded from device.
  - Different user : user whose user information in BioAdmin software doesn't correspond to user information uploaded from device.
  - New user : user information uploaded from device doesn't exist in BioAdmin software. it can be construed as surplus user in device.
- Color classification
  - Same user : indicated in yellow.
  - Different user : indicated in red.
  - New user : indicated in white.
- Check classification
  - Check all: check (select) all user information
  - Uncheck all : to uncheck after checking all user information
  - Check reverse : to uncheck checked user or check unchecked user
  - Delete selected user : to delete selected user
  - Check same users : select users whose user information in BioAdmin software corresponds to user information uploaded from device.
  - Check different users : select users whose user information in BioAdmin software doesn't correspond to user information uploaded from device.
  - Check new users : select users who are enrolled in device only but do not exist in BioAdmin software.
  - Delete all : to delete selected users and the other all users
- Hide same users

  If you press check same users, checkbox of a user whose data is same both in device and host PC is checked. If you display hide same users, these users can be hidden on finger scan information window.
- Get access group data

  Check a checkbox of get access group data and execute Get from device, to upload user access group information.

3.10. Synchronize all users

Synchronization all users button transfers all user data base in host PC to device and surplus users remaining in device only are deleted. User information such as user ID, fingerprint information, access group number and security level is uploaded thru this process.



Detailed operating process is as follows.

- Press **synchronize all users** button.
- Select applicable device on device list window.
- Press select button to transfer user information database in device from host PC to device.

> Note : By transferring all users to device, surplus users in devices will be deleted.

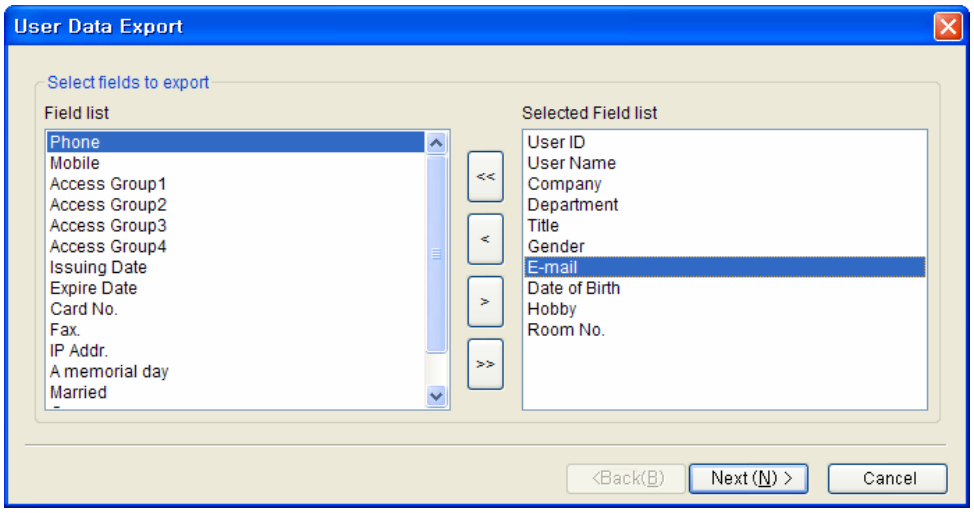
3.11. Export to file

The **Export to file** button initiates saving information of selected users in CSV format. Fingerprint templates are not included in this exportation. Exported CSV file

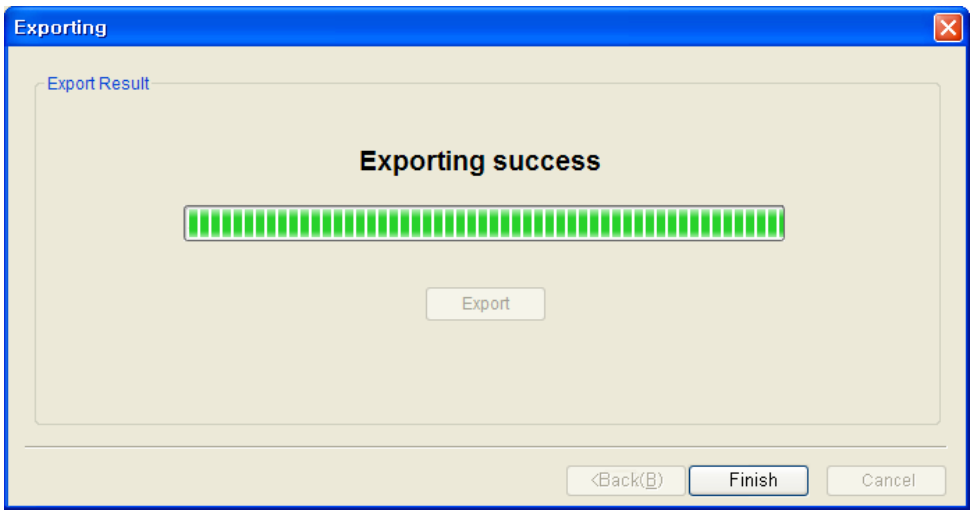
can be edited using Microsoft Office Excel or usual text editor.

Detailed operations are as follows.

- Check on the users to export.
- Press the **Export to file** 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.

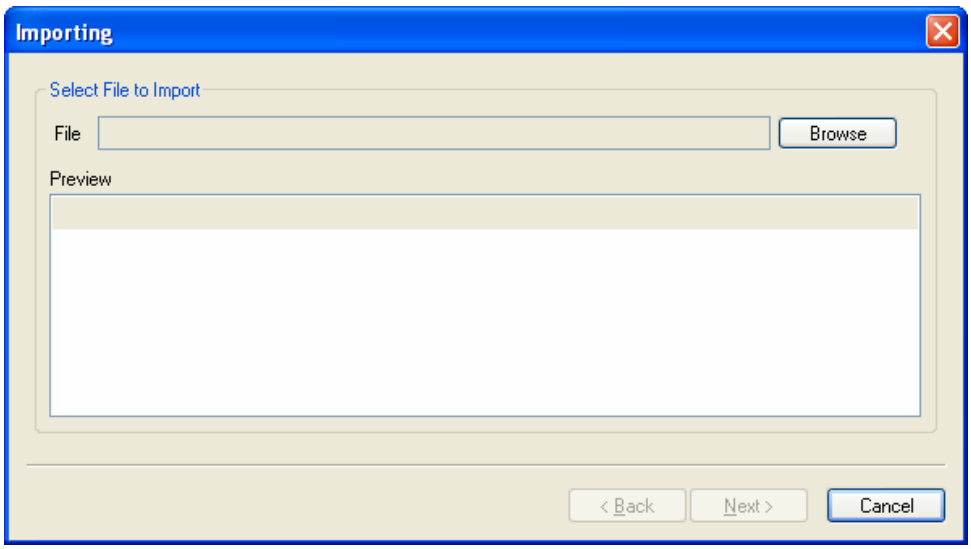


3.12. Import from file

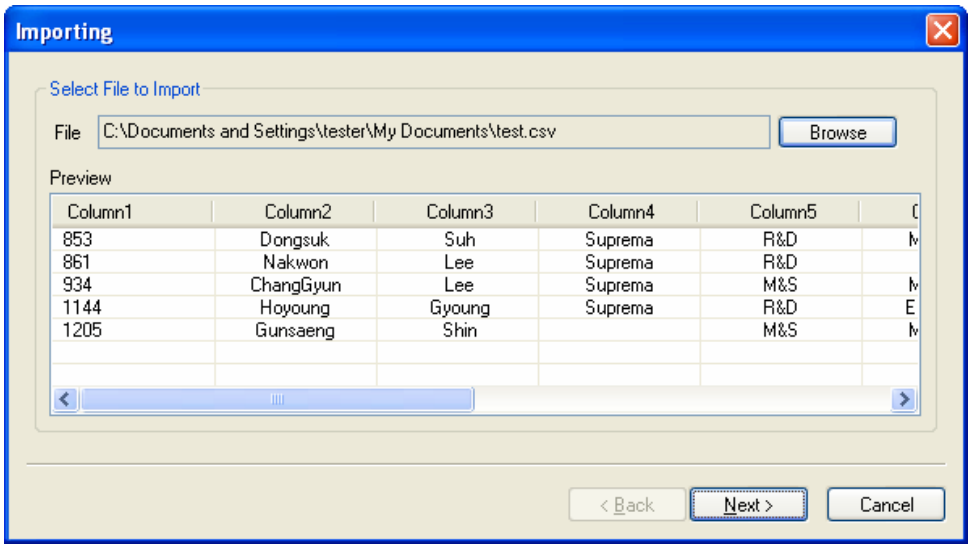
The **Import from file** button is used to upload user database from an external database to BioAdmin Software user database. User list saved as CSV (Comma Separated Values) format can be loaded into user database list.

Detailed operations are as follows.

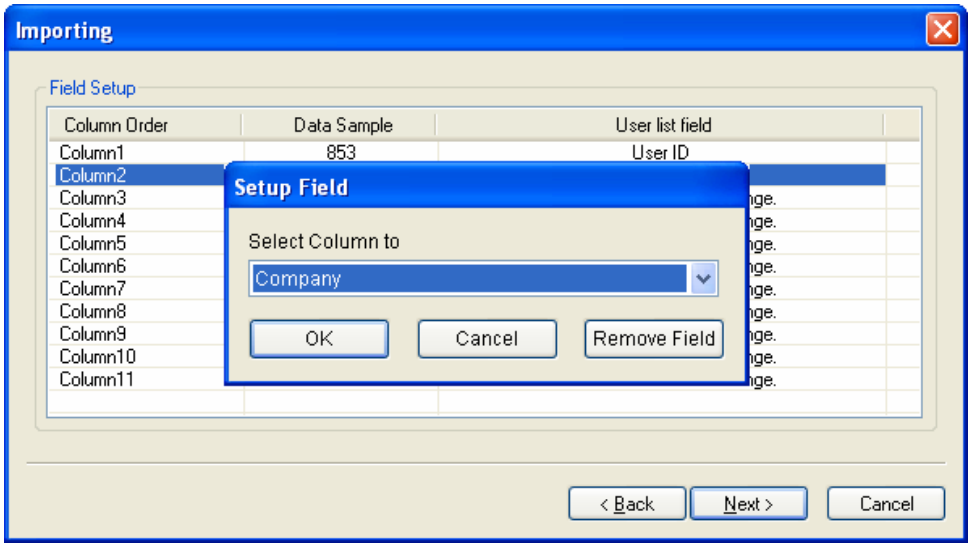
- Press the **Import from file** button.



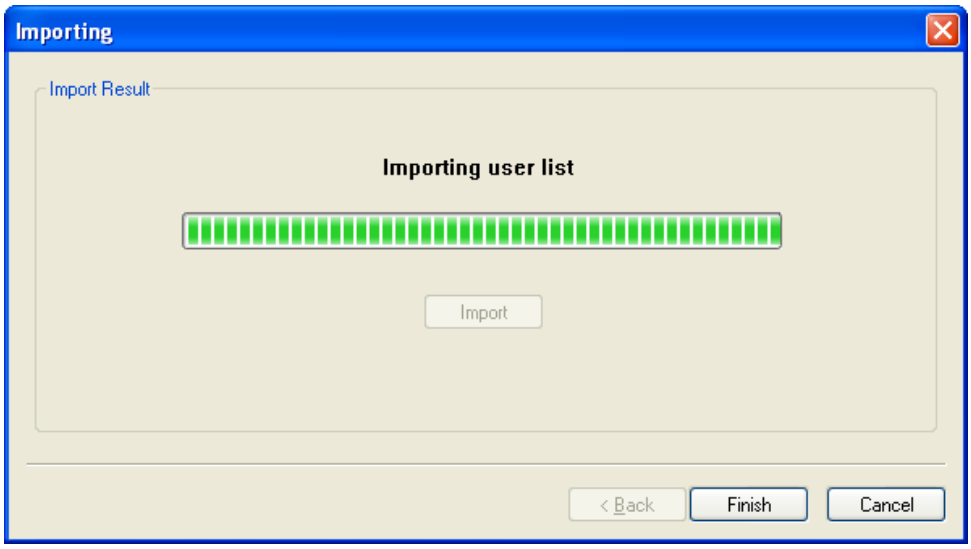
- Select a file to upload.
- After selecting the file, you can see the content examples of 5 users on the preview window. Check the preview window to confirm the selected file is the right file from which you want to upload the database.



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

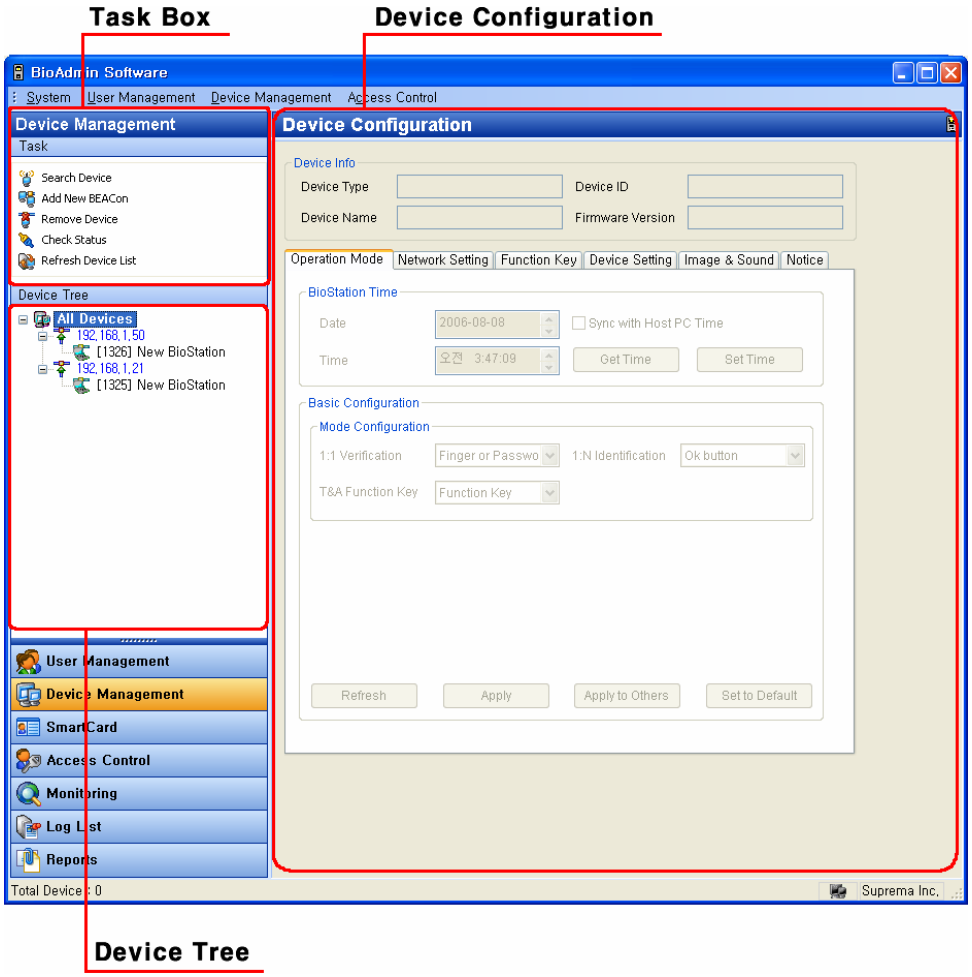


- Press the **Upload** button.



4. 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, BioStation, and BEACon. 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

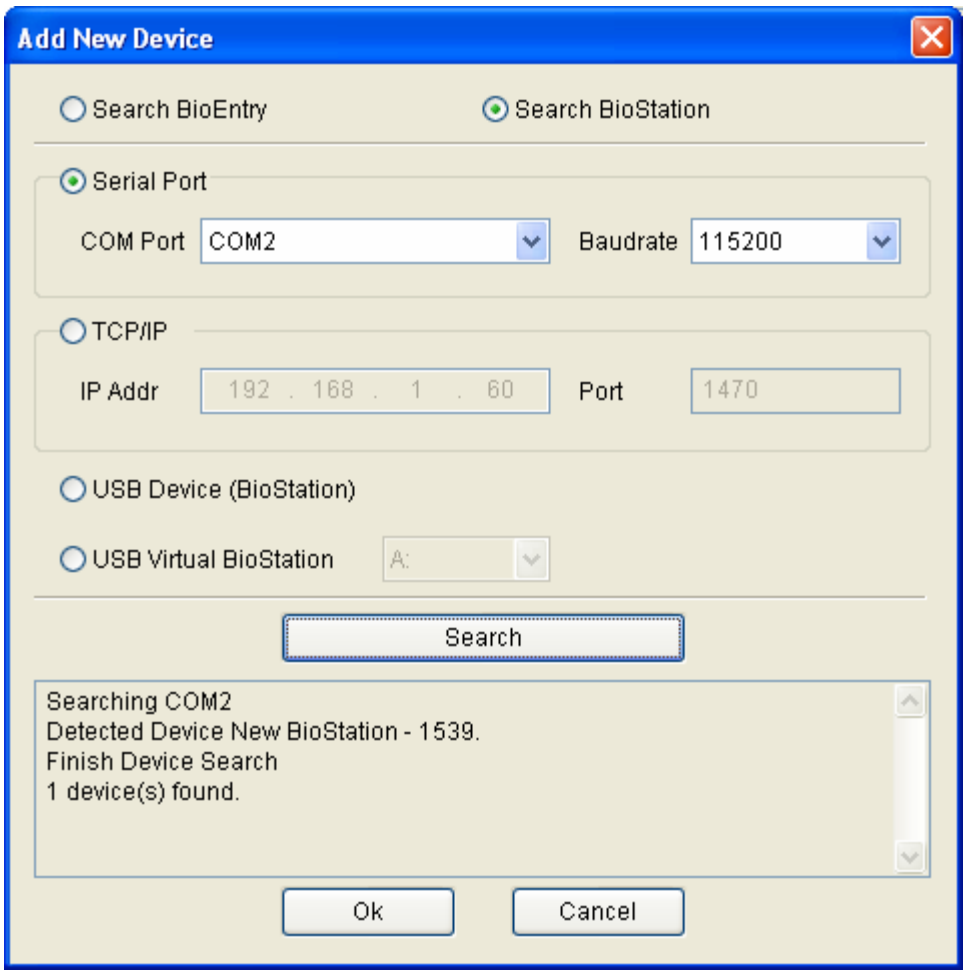
The Device Tree window shows the network condition of connected BioEntry, BioStation, and BEACon.

4.1. Search device

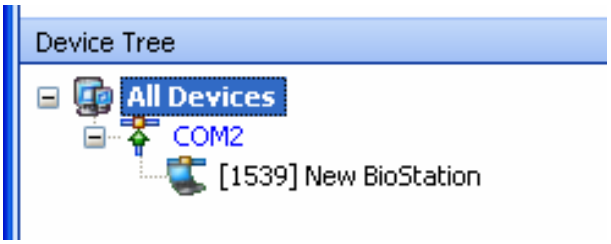
To search new BioStation or BioEntry device and add, click search device menu in task box. If add new device window pops up, select a device for search from BioEntry or BioStation and select serial port, TCP/IP (Ethernet) or USB device according to interface between device and host PC. Of these, USB connection is available only with BioStation.

4.1.1. Serial port

In case device and host PC are linked by serial network, set applicable COM port of host PC and select baudrate. Default baudrate of BioStation, BioEntry and BEACon is 115,200 bps.



Press search button to display search result. Press ok button to display searched device on device list. The number in bracket [ ] ahead of searched device name is device ID. To change device name, place a cursor on applicable device and press the right button of the mouse to display a menu. Choose 'change name' then input window appears where a new name can be entered.

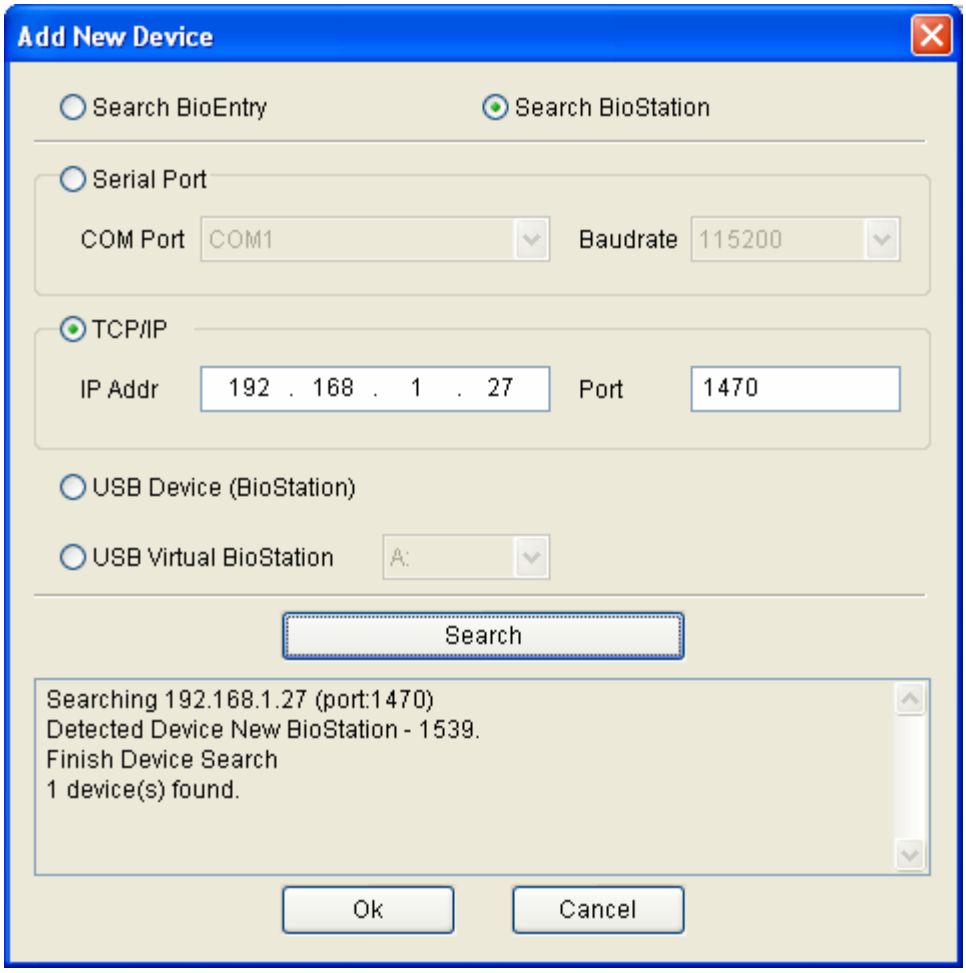


4.1.2. Ethernet

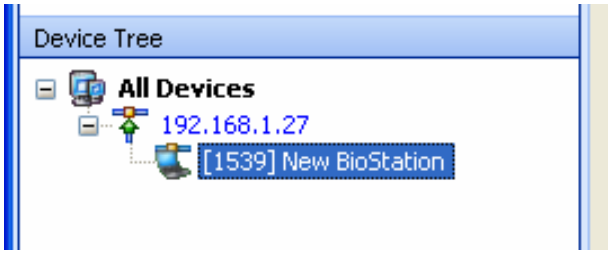
In case device and host PC is connected by Ethernet, enter IP address and pot in TCP/IP field on add new device window.

In case of BioStation and BEACon, IP address can be checked in device. For details, refer to manual of each device. In case of BioEntry, Ethernet interface is not supported but can be linked by Ethernet using Ethernet to Serial converter in host PC. Input IP address of mounted Ethernet to Serial converter.

Input 1470 for all ports.



Once device is linked correctly with network, searched device ID appears with bracket [****] under port on device tree window.



4.1.3. USB device

In case of connecting BioStation with host PC by USB, select USB device and search.

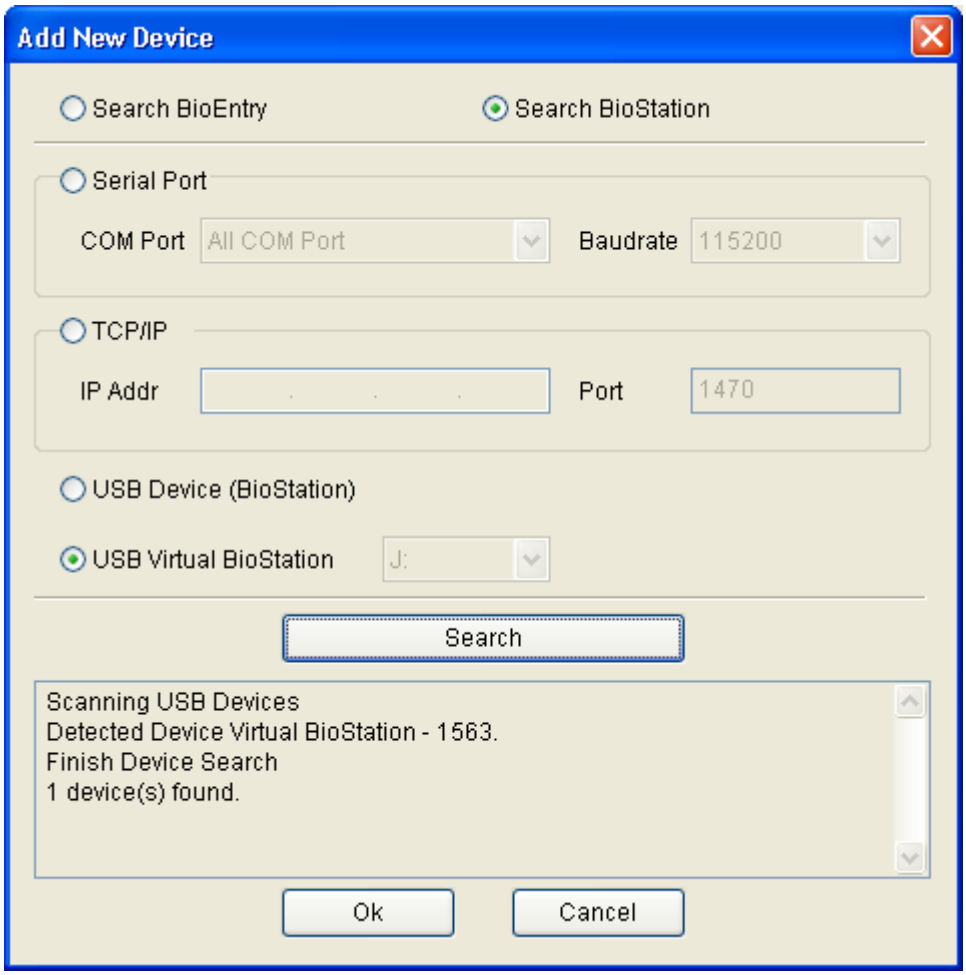
4.1.4. Virtual Terminal

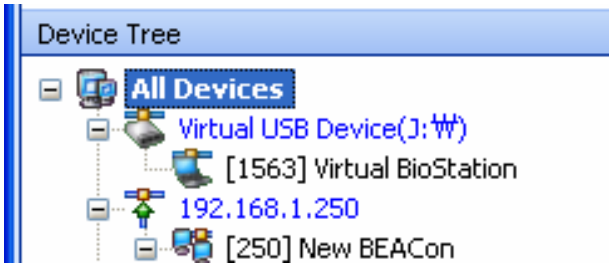
You can use a USB memory as a virtual BioStation terminal. After connecting a USB memory to BioStation, store the necessary information such as user information, log, and various setting values of the BioStation. Then, by connecting the USB memory to the host PC, you can utilize most of the BioAdmin menus with the connected virtual terminal.

> Note : To use a virtual terminal, OS of your host PC should recognize the USB memory as a correct USB drive. Thus, user should not change or remove the file in the USB drive.

You can add a virtual terminal to the network by the following procedures.

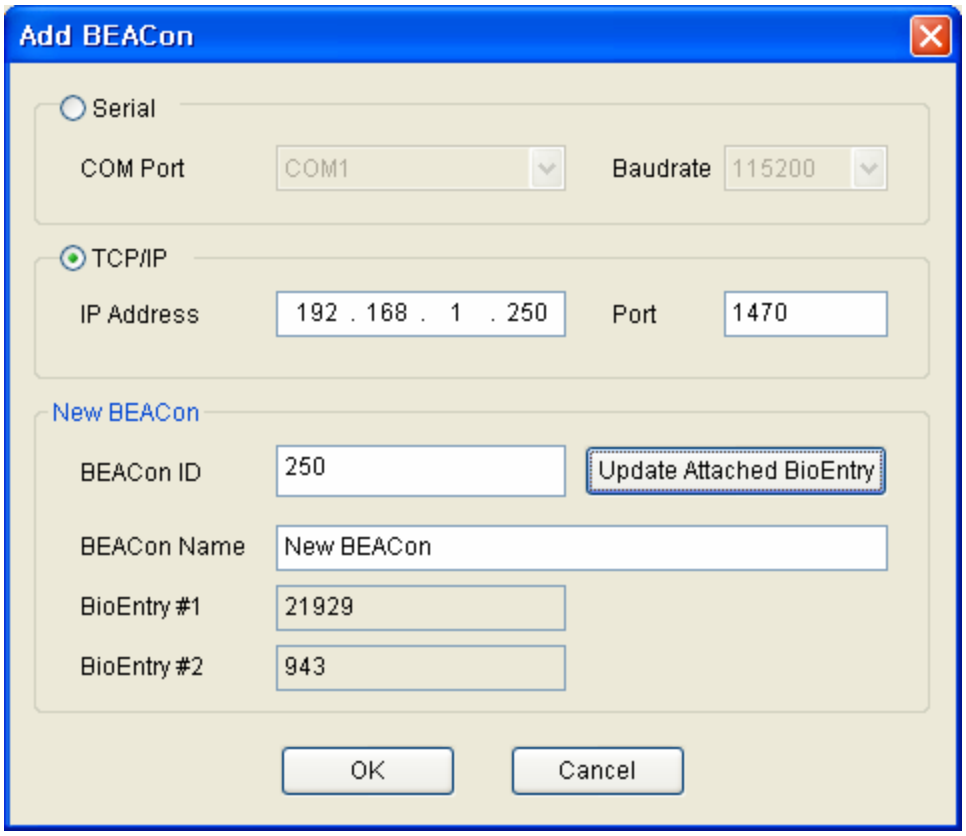
- Register a USB memory as a virtual terminal. You can do so with the **Initialize** menu of the Network / USB memory menu on BioStation. For the detailed operation, please refer to the BioStation User Guide.
- After registering a USB memory as a virtual terminal, connect it to the host PC.
- Check whether your host PC properly recognizes the virtual terminal as a drive.
- Select the virtual terminal on the **Search Device** menu.
- Select the drive of the connected virtual terminal and press **Search** button.
- After finding the virtual terminal, press **OK** button.





4.2. Add New BEACon

Searching and adding process of BEACon.

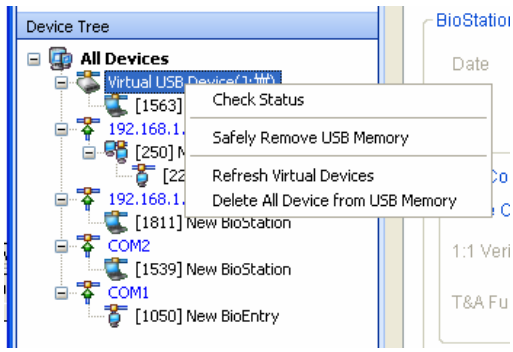


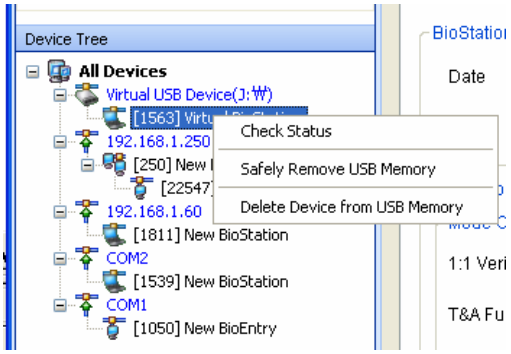
Detailed operations are as follows.

- Press the Add New BEACon button on the task box.
- Select the communication method between Serial and TCP/IP.
- In case of serial, set COM port and network baudrate and incase of TCP/IP, input IP address of BEACon to add. For how to check IP address in BEACon, refer to BEACon manual.
- Input BEACon ID to add in BEACon ID field. For how to check ID in BEACon, refer to BEACon manual.
- Designate and input BEACon name in Name field.
- If you press update attached BioEntry button, it starts searching applicable BEACon and linked BioEntry device.
- As a result of search, linked BioEntry ID is indicated in BioEntry #1 and BioEntry #2 fields. In case of failing to search BEACon due to wrong input of IP address or ID, none is indicated here.
- Press ok button to view searched BEACon and linked BioEntry on device list.

4.3. Remove device

- Select a device on task list and click **Remove Device** on task box to remove the selected device. You can also remove a device by selecting a device on device list and clicking a right button of the mouse.
- You can remove virtual terminal from the network by the following procedures.
  - Select a virtual terminal on the device tree and click the right button of your mouse.
  - Safely Remove USB Memory: Click this menu to detach the virtual terminal from your host PC after storing data on it. If you detach the virtual terminal while storing or using data, it can cause a data loss from the virtual terminal
  - Delete All Device From USB Memory: Remove the data of all virtual terminals from the USB memory. To use the USB memory again as a virtual terminal, you need to register the USB memory as a virtual terminal.
  - Delete Device from USB Memory: Remove the data of the selected virtual terminal from the USB memory.

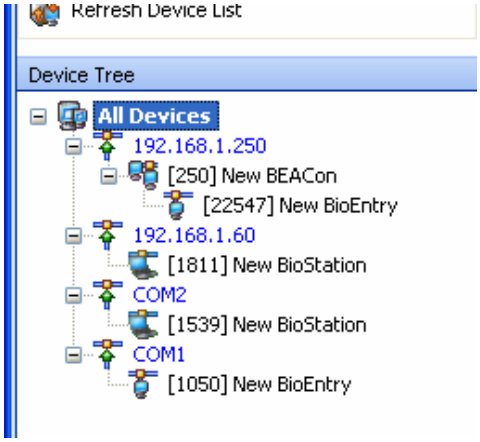




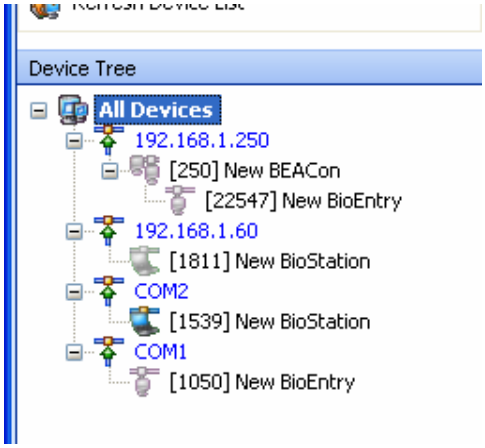
4.4. Check status

Device's current status is classified by device icon on device list window.

- If a device is connected, icon is active.



- If a device is not connected, icon is inactive.

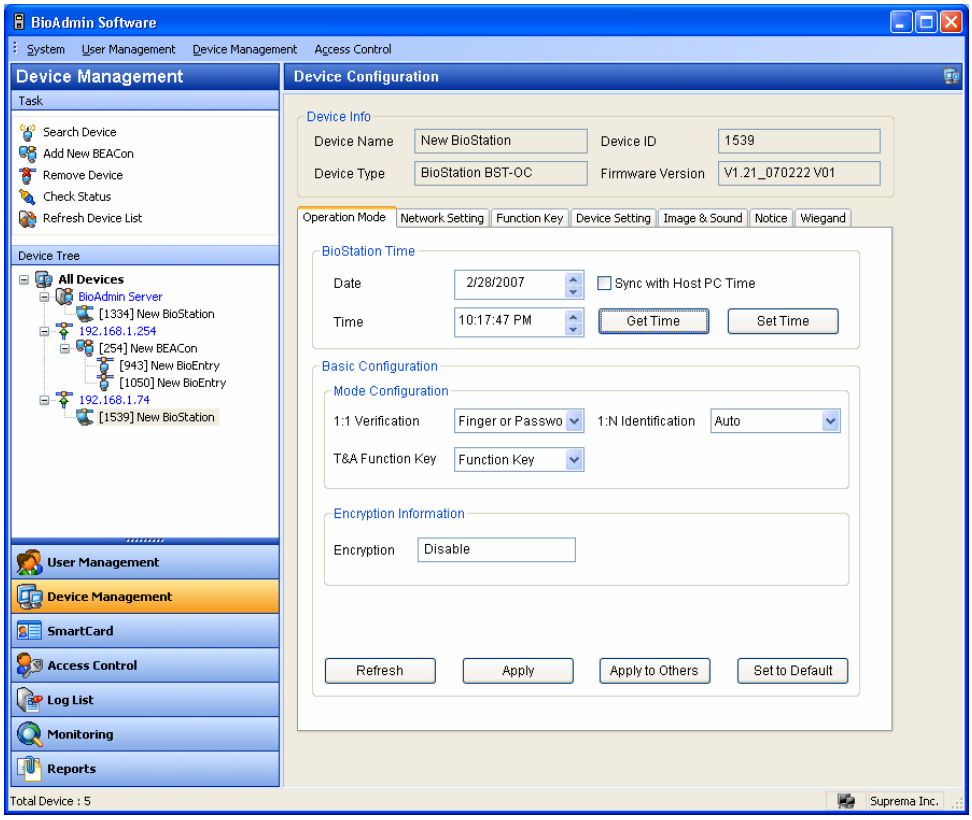


Status of each device is updated in case of the followings.

- When BioAdmin software starts
- When a device is selected anew
- When clicking check status menu
- When connecting BioStation to host PC via USB

4.5. Manage BioStation device

If you select BioStation on device list, the device setup window of selected BioStation is updated on main window.



Device setup window is divided into 2 areas.

- Device information

  Device information displays type, name, serial number and FW version of selected device.

- Configuration window

  Configuration window shows settings of selected BioStation device and enables user to correct those settings. Configuration menu consists of separated tabs, i.e. operation mode, network, setting, function key, device setting, image & sound, and notice.

  At lower part of configuration window are 4 buttons, i.e. refresh, apply, apply to others and set to default.

  - **Refresh** : call device setting again.
  - **Apply** : apply corrected setting on the current window to device.
  - **Apply to others** : apply corrected setting on current window to another device. Device can be selected on select device window.

- **Set to default** : change setting as default. To apply this value to device, make sure to press apply button.

4.5.1. Device information

You can check device name, device type, device ID and firmware version of selected BioStation. Device ID number and firmware version are necessary information to check a product for technical support after installation.

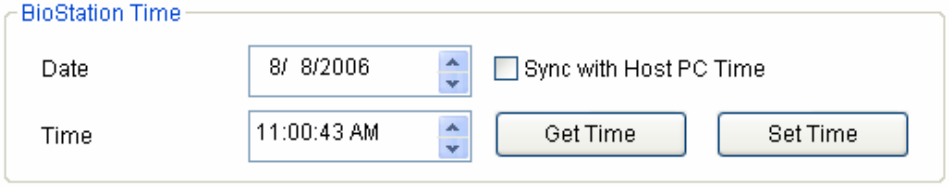
4.5.2. Operation mode

- Time setting

  Date and time shown first are those read from BioStation. If you click get time button, it reads date and time from BioStation once again.

  Method of BioStation time change is divided into direct input and synchronization with current PC time.

  - Direct input : either input numbers directly in date and time window or place a cursor on a number and click up/down arrow keys for input. Press set time button after input to transfer input date and time to the selected BioStation.
  - Synchronization with PC time : check **sync with current PC time** and set time button, then selected BioStation time is set by current PC time.



- Mode setting

  1:1 verification : if you select 1:1 verification on BioStation, user ID should be suggested first and then the user should authorized himself with his fingerprint or password.

1:1 verification	How to suggest User ID	How to authorize
Finger or Password	Enter User ID or Put the card	Put finger or enter password
Finger Only	Enter User ID or Put the card	Put Finger
Password Only	Enter User ID or Put the card	Enter password
Card Only	Put the card	

Finger or Password : User should suggest his User ID by entering User ID on the keypad or by putting his card to the BioStation RF. After suggesting his User ID, user should verify himself with his fingerprint or password.

Finger Only : User should suggest his User ID by entering User ID on the keypad or by putting his card to the BioStation RF. After suggesting his User ID, user should verify himself with his fingerprint.

Password Only : User should suggest his User ID by entering User ID on the keypad or by putting his card to the BioStation RF. After suggesting his User ID, user should verify himself with password.

Card Only : User can verify himself only by putting his card to the BioStation RF.

- 1:N identification : in 1:N identification, user is authorized by fingerprint without user ID input. About how to start fingerprint input, user can choose one of 3 modes, i.e. auto, OK button and none. In **auto** mode, because BioStation sensor is always on as standby mode, scan starts right after a finger is placed on the sensor. If you choose **OK button** mode, place a finger after pressing OK button on BioStation when entering fingerprint. In

case of not using 1:N mode but using 1:1 mode only, choose none mode.

- T&A function key : T&A function key is to enter T&A event before entering fingerprint for T&A control such as in, out, in duty, out duty. In BioStation, usually from F1 to F4 function keys are used for this and, if necessary, function key can be increased up to 16 keys. T&A key mode can be chosen from **function key** mode and **none** mode. In case of using BioStation for exclusive use of access control, choose none while in case of using for T&A control, choose function key. Pressing T&A key on BioStation first and then enter fingerprint to record applicable T&A event in a log. In the future T&A software, this log information can be used for various T&A and salary control data.

In case of changing settings such as various modes, changes are applied only after apply button is pressed. For detailed explanation on buttons at lower part of a window, refer to the previous page.

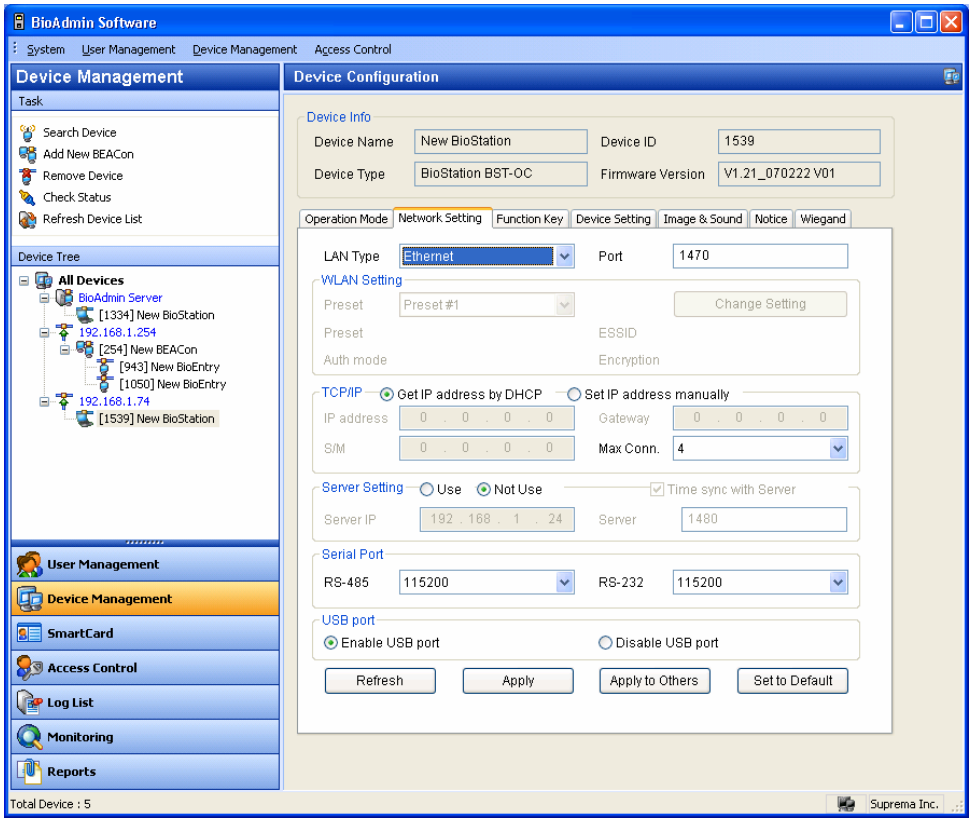
- Encryption Information
  - Encryption: if you use encrypted template, encryption is Enable.

4.5.3. Network setting

This window shows setup for various networks of a device. As per interface methods, it is divided into LAN, serial, and USB.

- LAN

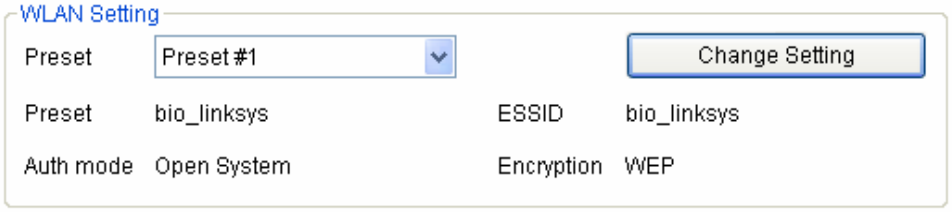
  In network setup list box at upper part of a window, set whether or not to use LAN and if yes, whether to use cable LAN or wireless LAN. Specify a port as 1470.



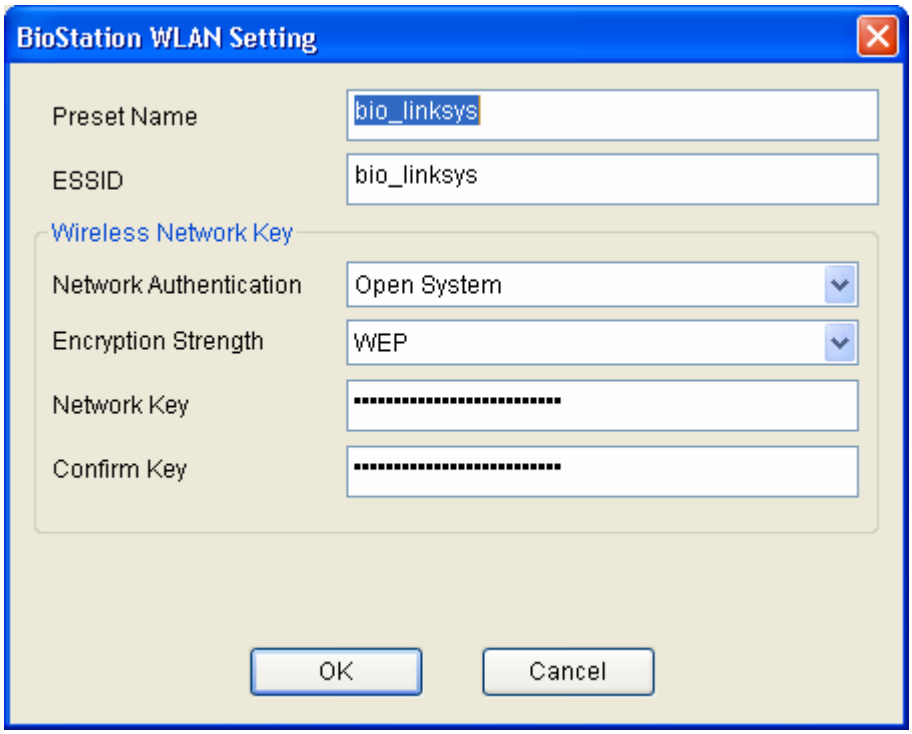
- Setup wireless LAN

  To setup the wireless network, you need the following procedures.

  First, you need an access point. Each access point has its own SSID, and, in some cases, it use the data encryption. BioStation supports WPA_PSK and WEP as the data encryption methods. Refer to the manual of your access point device and check whether it is using the data encryption. If yes, you need to check the type of the data encryption.



  - Preset: To activate the wireless network, you should select one of the 4 preset. Of course, you can not use the wired LAN upon using wireless LAN function.



- Preset Name: preset name is displayed on the BioStaiton using WLAN setting.
- ESSID: ESSID is the unique ID of the access point. To check the ESSID of your access point, refer to the manual of your access point or ask your network administrator.
- Auth mode: You can select the network authentication open system, shared key and WPA-PSK. It must have same setting to authentication of access point. You can see this setting on security page in access point setup application.
- Encryption Strength: You can select the encryption strength between WEP and WPA-PSK. By selecting WEP or WPA-PSK, you can encrypt the communication data between access point and BioStation.
- If the BioStation is too far from the access point, or there is an obstacle between BioStation and access point, the network can be interrupted. Also, the wireless network may not be successful due to the unique characteristics of the access point. Thus, it is highly recommended to have another network method rather than wireless LAN.

- Setup cable LAN

In BioStation settings, choose whether to get IP address automatically or set manually.

In case that IP address is automatically assigned to DHCP in BioStation, check 'get IP address automatically'. In case of not using DHCP, check 'set IP address manually' and set IP address, gateway, subnet mask and DNS. Changing LAN setting like this is required to set IP address in order to connect Serial or USB linked BioStation by LAN or to change IP address of BioStation connected by LAN to another address.

Max Conn means the maximum number of host PCs. Server-Client application is available only when the system is networked through Ethernet. If the system operates as server-client, users can operate the BioAdmin Client program from multiple host PCs. However, if the system is not operated as BioAdmin Server-BioAdmin Client but connected just as normal Ethernet, there will be a limit to the maximum number of host PCs to operate BioAdmin at the same time. For example, if you select this menu as 4, you can operate the BioAdmin program on 4 host PCs at the same time.

- Server Setting

  This menu shows that the BioStation is connected to the server.

  You can connect the BioStation to the server by checking on Use option and entering the server IP and server port.

  If you connect a BioStation to the server, existing Ethernet connection of the BioStation is disconnected and the BioStation is connected to the server. It may take a few minutes to reconnect to the server depending on the network condition.

  If you check on the **Time sync with Server menu,** the time of BioStation will be automatically set as the time of the server.

  If the network between a BioStation and BioAdmin Server is not stable, you can reconnect the BioStation to the server. Select the BioAdmin Server on the device tree window of Device Management menu and press the right button of your mouse. Press the **Reconnect Server** menu. You can also find this **Reconnect Server** menu on the System menu of Command Menu Bar.

- Serial

  Set baudrate of BioStation's RS485, RS232 ports. Default is 115,200 bps. As to serial, in case of any trouble in condition of cable, lowering baudrate can be a solution.

- USB connection

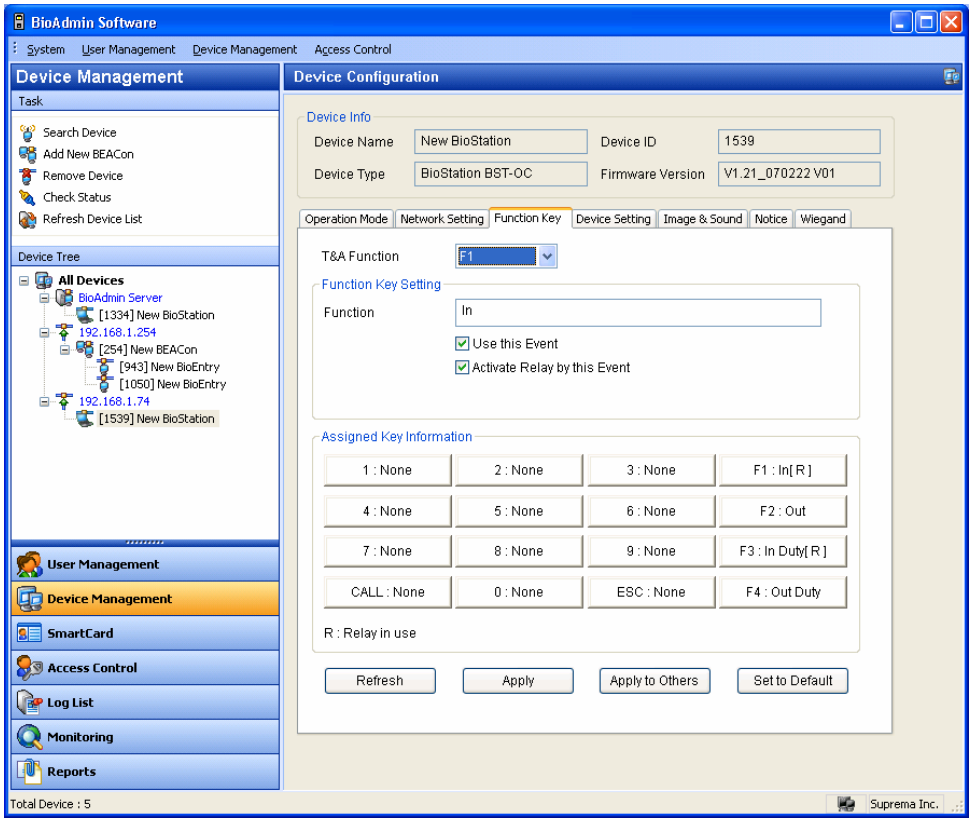
  Select whether or not to allow connection with host PC via USB port of BioStation. As USB port is exposed to outside, in some cases, connection is not allowed for security reason.

4.5.4. Function key

Function key is to input T&A event before fingerprint input for T&A control such as in, out, in duty or out duty. In BioStation, usually, function keys from F1 to F4 are used and if necessary, it can be increased up to 16 keys. Pressing function key on BioStation first and then enter fingerprint to record applicable T&A even in a log. In the future T&A SOFTWARE, this log information can be used for various T&A and salary control data.

In respect of function key in BioAdmin software, reference needs to be made to all explanations on T&A event rule in both device management menu and report menu.

Function key setting in device management menu is to set T&A event message shown on BioStation display whereas T&A key setting in repot menu is to set T&A event message applied when creating T&A report. In BioStation log, actual T&A event message is not recorded but the number of pressed T&A key is recorded. BioAdmin reads this value, refers to the table between previously defined function key and T&A event and generates suitable T&A report. Thus, function key set in this chapter doesn't show in an actual BioAdmin report or upon log check.

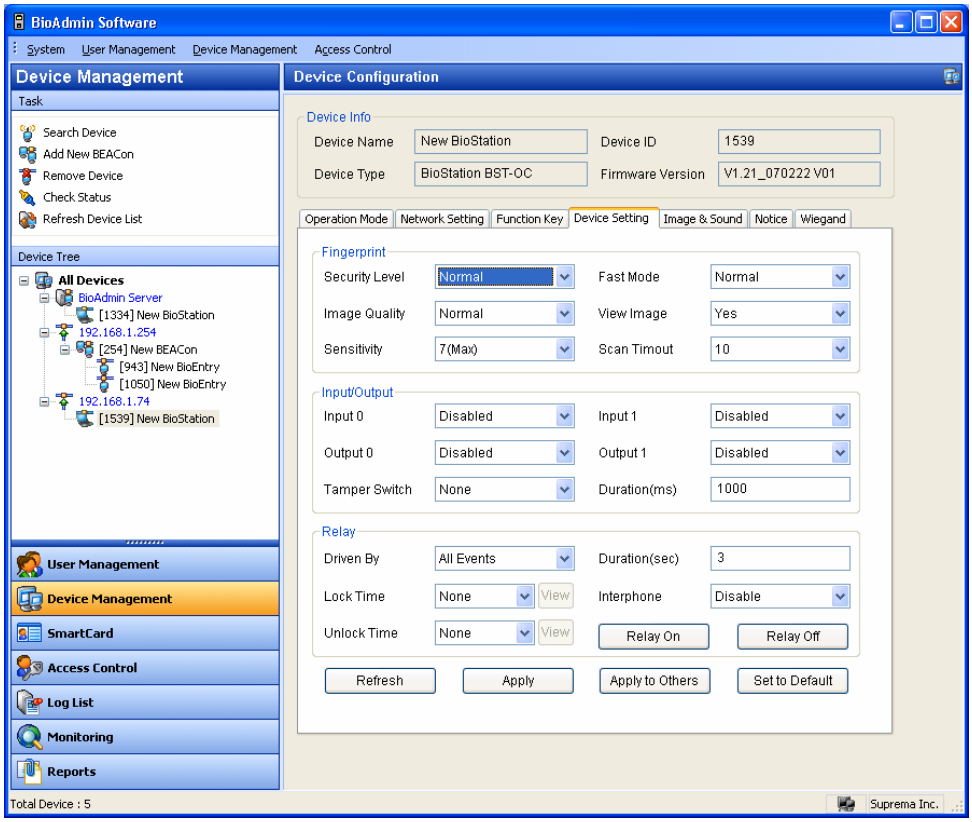


Set 16 keys in device and choose one out of 16 function keys to check function key event message displayed on BioStation LCD, use of this function key and relay use.

- Choose a function key to set.
- Enter event name in **function** field.
- Decide whether or not to check **use this event**.
- Decide whether or not to check **activate relay by this event**. Relay is usually linked to door lock control device and used to open/close a door.

4.5.5. Device Setting

This window is to check and change various settings of BioStation



- Security level

  Security level can be chosen among normal, secure, and most secure. Internally security level adjusts FAR(False Acceptance Ratio). As FAR and FRR(False Rejection Ratio) are in inverse proportion to each other, the higher security level is the more FRR increases, so does FRR. Default is normal.

- Image quality

  Decide standards by which the quality of input fingerprint image is over certain level. You can choose from weak, normal, and strict. Default is normal.

- Sensitivity

  Sensitivity decides sensitivity of detecting a finger. In high sensitivity, finger input is accepted more easily but if sensitivity is lowered, input fingerprint image gets more stable as fingerprint is captured only when fingerprint covers more than a certain part of a finger. In case of optical model, sensitivity can be moderated by lowering setting of sensitivity against the rays of the sun. Default is 7 (Max)

- Fast mode

  In case more than hundreds fingerprints are saved in device, 1:N mode may

take longer. If you set fast mode as fast or fastest, performance is somewhat low but 1:N recognition can take less time. Default is normal.

- View image

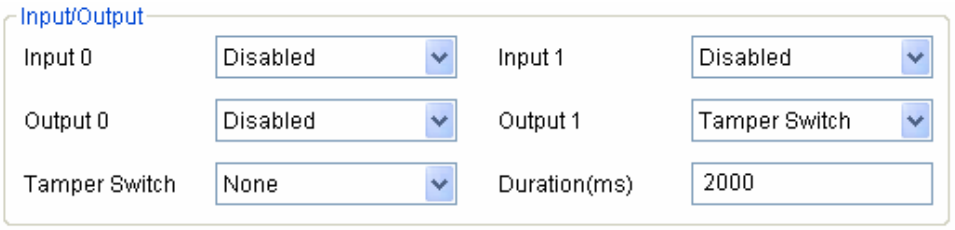
  User can choose either to yes or no to view or hide input fingerprint image on LCD display of BioStation. Default is yes.

- Scan timeout

  User can designate the standby time when entering fingerprint. If a user doesn't enter fingerprint within this time, it is construed as input failure. Default is 10 sec.

- Input/Output setting

  BioStation provides 2 respectively programmed input and output which can be connected to external device. In input/output menu, set input/output port.



  - **Input port setting** : 2 ports of input 0 and input 1. Choose from exit switch and disabled.
  - **Output port setting** : 2 ports of output 0 and output 1. Choose from duress, tamper switch, authentication success, authentication failure, and disabled. Signal output time of output port can be set in msec unit.
  - **Tamper switch** : in case BioStation case is open, choose whether or not to set system lock mode for security reason.
  - **BioStation relay setting (driven by)** : user can change relay setting in BioStation. Choose from all events, selected events and disabled. In case of all events and selected events, user can set door open time.
  - **Open time/close time** : door open time and close time can be set separately by day / holiday group. It should be set in advance in time zone setting on access control menu.
  - **Duration (sec)** : relay running time as per set event. Once door is released, door can be locked again after set door open time.
  - **Interphone**: Enable this option when you are using a interphone along with BioStation.
  - **Relay On / Off** : Administrator can control the relay of the BioStation by

using this Relay On/Off menu.

> Note : overall system door open time is computed by adding door lock open time and device open time.

4.5.6. Image & sound

Menu to set background, sound effects and other display/sound of BioStation. User can set desired background, notice and log image and also change sound effect fit for user's style.

- Change background

  In this menu, user can change background image of BioStation. BioStation background can be chosen from logo image, slideshow, and notice. Image file format which can be uploaded to background are varying, i.e. JPG, GIF, BMP and PNG but size is fixed as 320*240 pixels. In case the size of image file to upload is different, adjust image size using graphic tool.

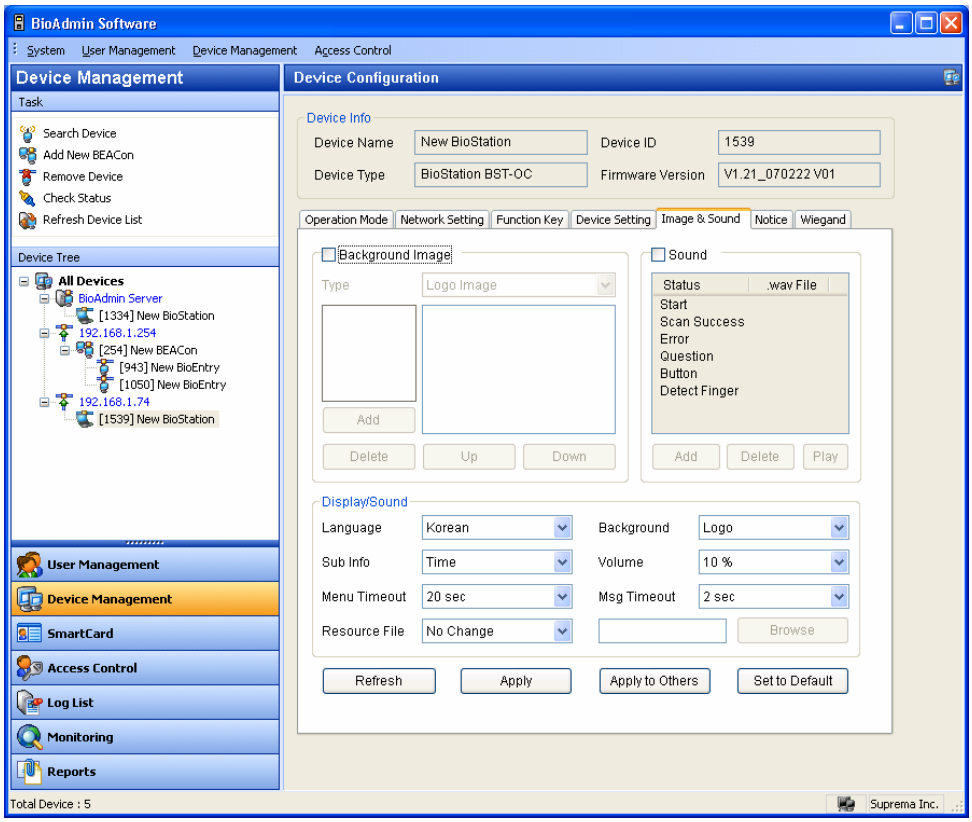
  In background, user can choose and upload one image file as background of logo image and notice. As for slideshow, maximum 16 image files can be uploaded and it shows images in turn at a set interval.

- Change sound effects

  In this menu, user can change sounds of device or check current sound effects. Sound effects of device consists of 6 sounds in total, i.e. start sound when device is turned on, button sound when pressing a button, scan success sound when finger scan is successful, question sound when pressing a ESC button, error sound when finger scan failed, detect finger sound when a finger is placed on fingerprint sensor.

  > Note : the size of sound file can't exceed 512KB and sounds may not change depending on the format of the file.

- Display/sound setting
  - **Language** : choose language used for menu and various messages on BioStation LCD display. Language can be chosen from Korean, English and Custom.



- **Sub information** : set items displayed at the lower part of BioStation background. Choose from notice, time, and none. In case of notice, contents are scrolled from right to left on display. Default is time
- **Menu timeout** : if no input is made in a certain menu for a set time, it returns to initial page. Choose from infinite, 10 sec, 20 sec, 30 sec. Default is 20 sec.
- **Resource file** : choose from English, Korean, Custom, no change. Select language to change, click browse and choose applicable configuration file(*.rc) after changing configuration file, reset BioStation to apply and select applicable language on language select menu to view.
- **Background** : Choose from logo, notice and slideshow as background of BioStation LCD display.
- **Volume** : to adjust speaker volume of BioStation. Volume ranges from 0 to 100%. When using daily in normal situation, set a volume as 20-50%. Default is **20%**.
- **Msg Timeout** : When a user matches his fingerprint, BioStation shows the success or fail message on its screen. Administrator can change the time

during which those messages are shown on the BioStation. Default is set as 2 seconds.

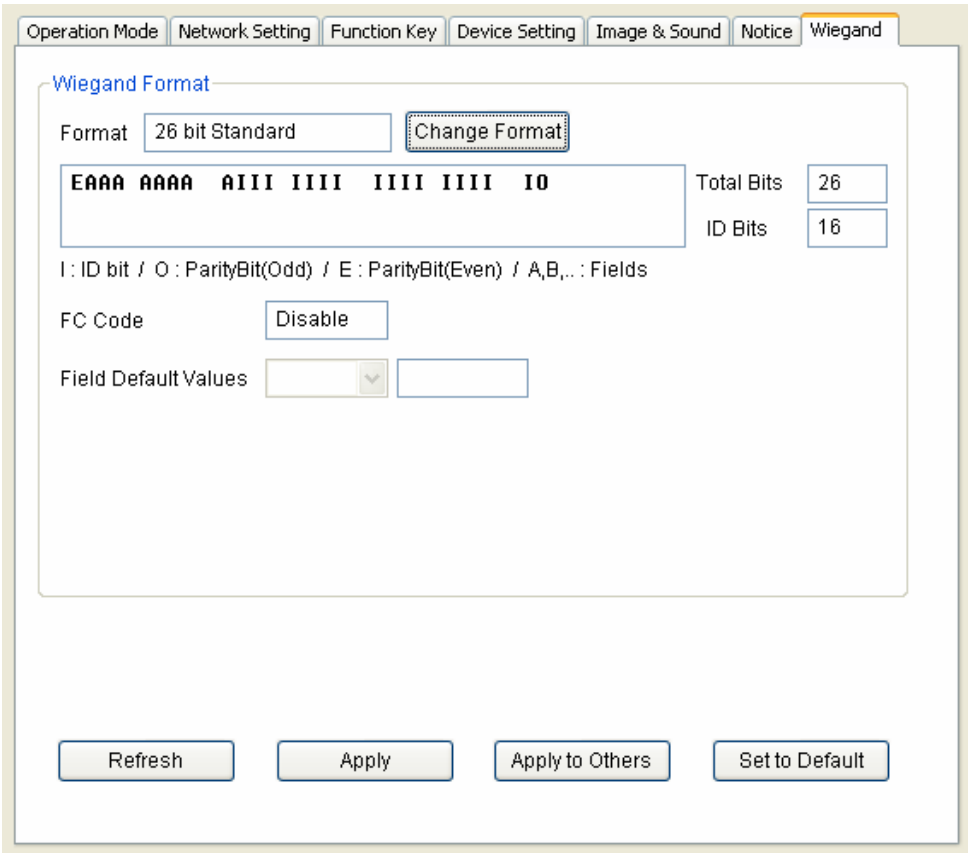
4.5.7. Notice

If there's company notice, administrator can show the notice on LCD of BioStation. Notice can be input up to maximum 1024 byte and a number of letters varies depending on language.

After transferring notice to device by pressing apply button, you can check and view notice on LCD of BioStation only if you selected notice as background in display/sound menu and apply.

4.5.8. Wiegand Setting

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

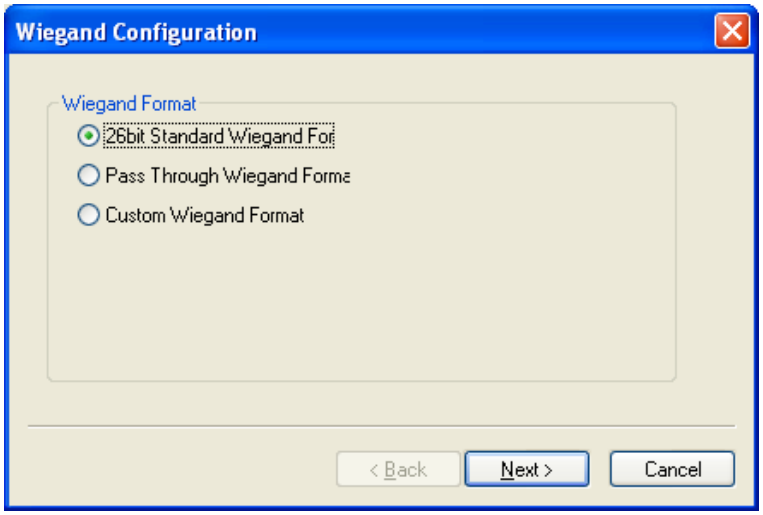


- Wiegand Format

  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.



- 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

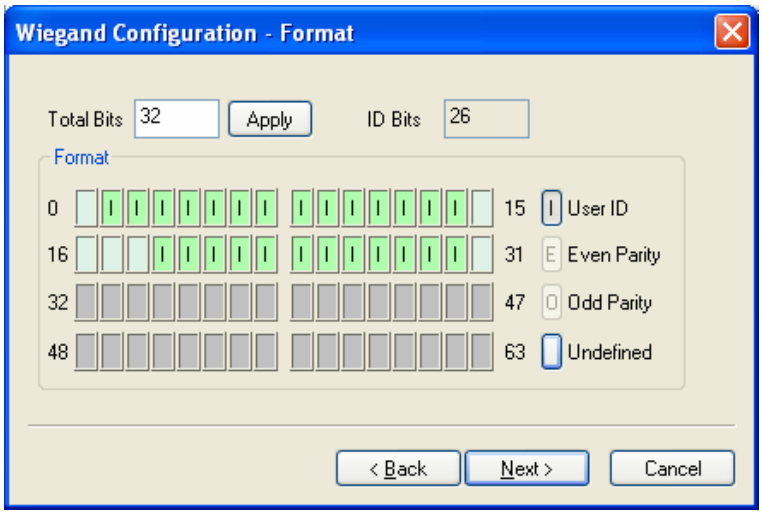
  Pass Through format is used when only the format of ID field is known. When the Wiegand input string is detected, BioEntry device extracts ID bits and starts verification with the ID. If the verification succeeds, the device outputs the Wiegand input string as unchanged. Parity check and advanced options 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.

- 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 device checks the parity bits first. If all the parity bits are correct, the device 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 device 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 IIIO

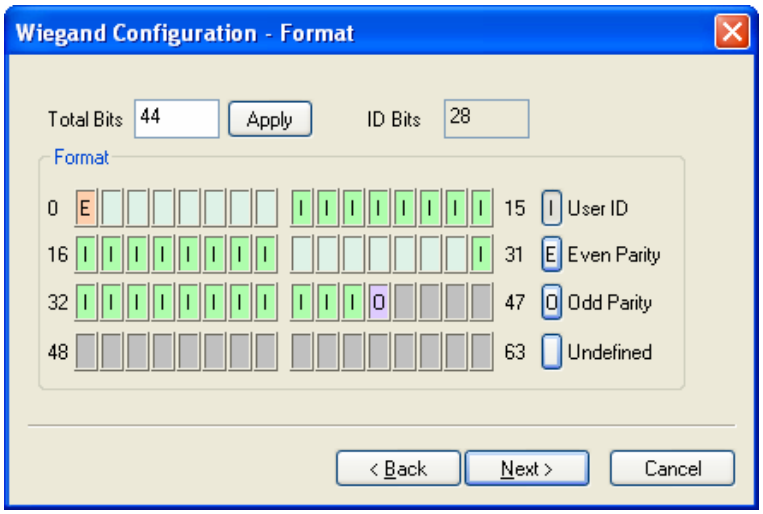
  (left most bit is 0th bit, BIT0)

  E: Even parity for BIT1 ~ BIT22

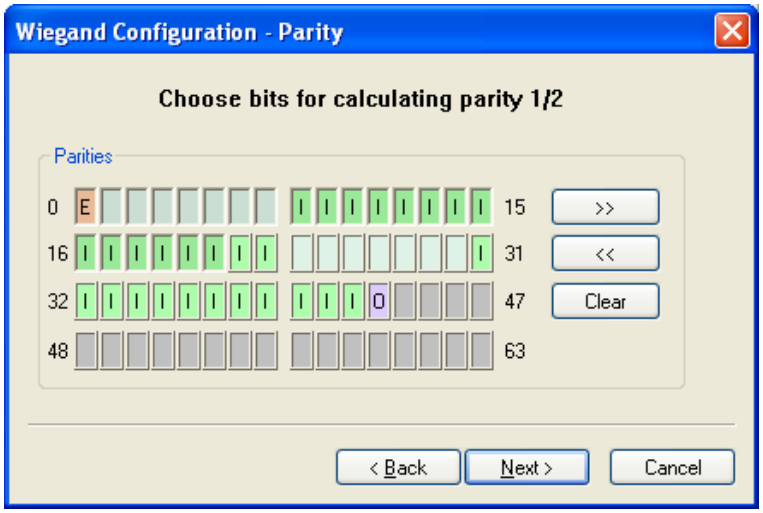
  O: Odd parity for BIT23 ~ BIT42

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

  You can configure this format in the following sequences.



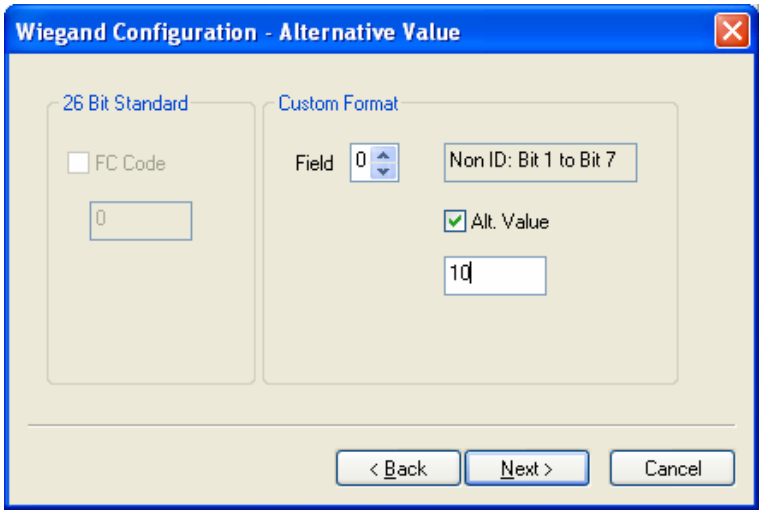
- Enter 44 in the **Total Bits** field.
- Select **Even Parity**.
- Press the even parity bit. In this example, it is BIT0.
- Select Odd Parity and press the odd parity bit and User ID according to the definition.
- Press **Next**.



- Press the bits which are used in calculating the first parity bit. In this example, they are BIT1 ~ BIT22
- Press >>.
- Press the bits which are used in calculating the second parity bit. In this example, they are BIT23~ BIT42.
- Press **Next**.

- 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™ device will replace corresponding fields with these values before sending outputs.



4.6. Manage Virtual Terminal

You can manage a virtual terminal with the same device management menus for BioStation, except the followings.

- Time Setting : You can not set the time of BioStation with virtual terminal. Thus, you should set time directly to BioStation.
- Lock all devices / Unlock all devices : You can not set lock/unlock of BioStation with virtual terminal. Thus, you should the lock/unlock directly to BioStation.
- Firmware Upgrade : Store a firmware file on a virtual terminal. Connect the virtual terminal to BioStation and upgrade the firmware using firmware upgrade menu on BioStation.

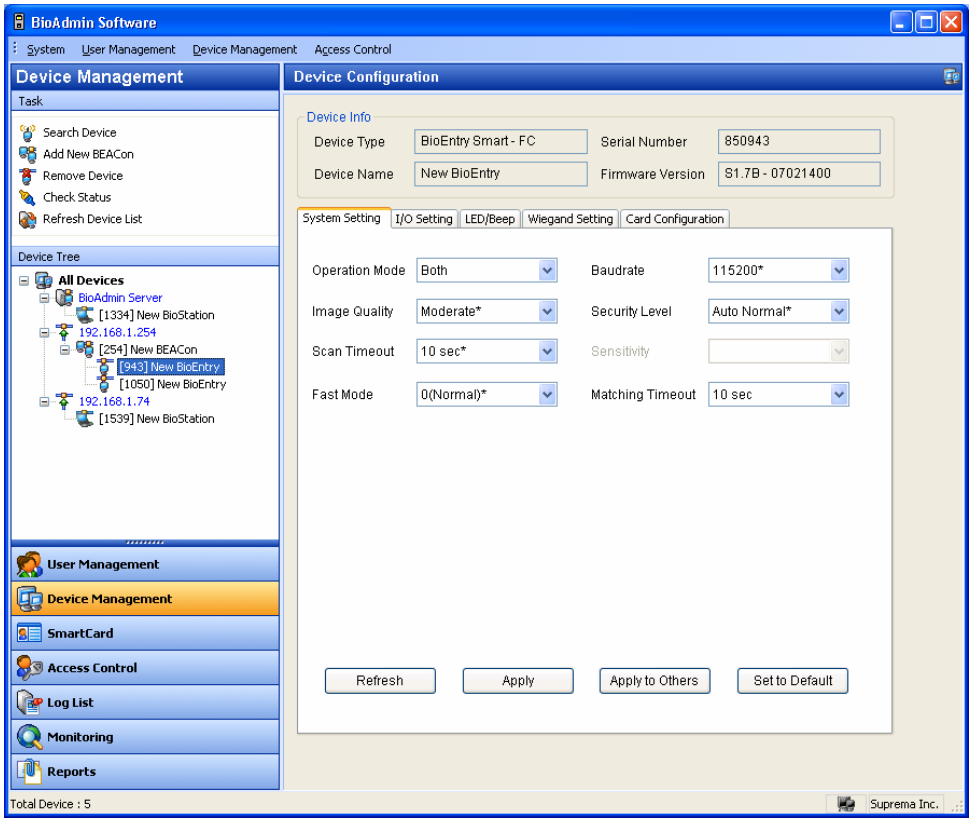
After connecting a virtual terminal to BioStation, you can use the following menus of BioStation. For the detailed operation, refer to the BioStation User Guide.

- Synchronize : Change the user data and device settings of BioStation as same as the stored data on virtual terminal .
- Export Virtual Terminal : Remove the stored data on virtual terminal and make a new virtual terminal with the current data of the BioStation.

- Import Virtual Terminal : Remove the stored data on BioStation and apply the data store on virtual terminal.
- Firmware Upgrade : Upgrade the BioStation firmware with the stored firmware file on virtual terminal.
- Initialize : Remove all virtual terminals on from USB memory.
- Refresh : Check the status of the USB memory and activate menus regarding USB memory.

4.7. Manage BioEntry device

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, and Card Layout.

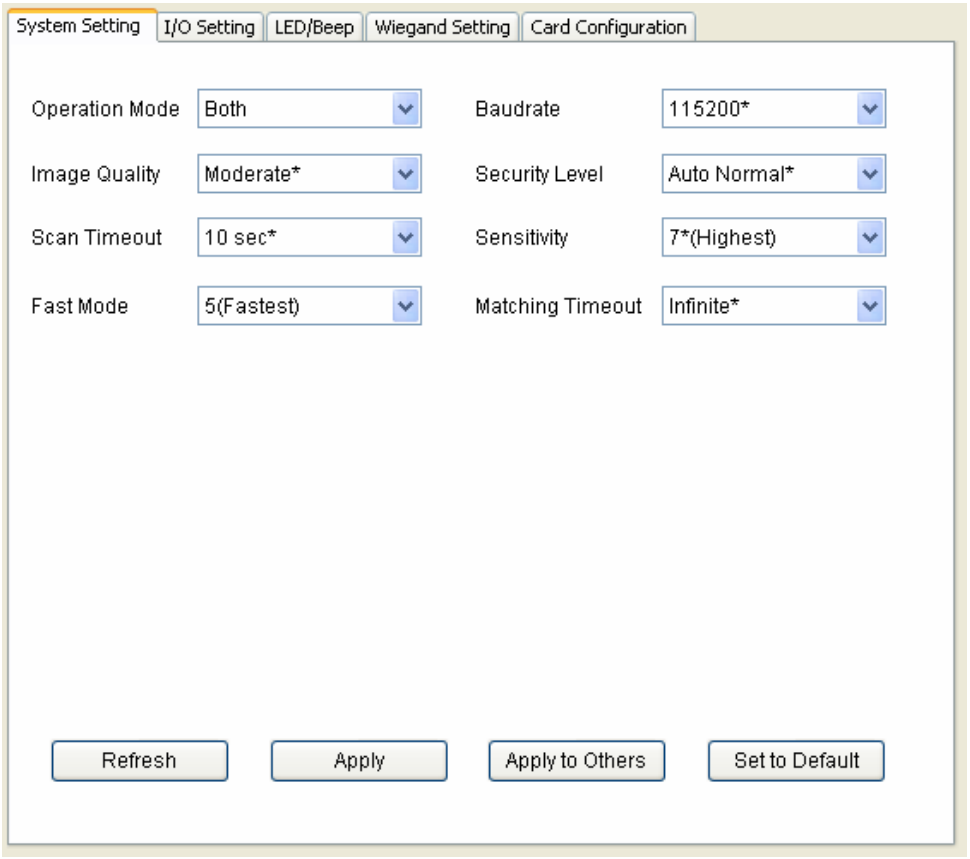
4.7.1. Device information

Administrator can check device name, device type, device ID and FW version of

BioEntry. Device ID number and FW version are necessary information to check a product for technical support after installation.

4.8. System Setting

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



- Operation Mode
  - 1:1 verification : if 1:1 mode is selected in BioEntry Smart, present user smart card first and finger scan starts. In case of BioEntry Pass, finger scan is processed by Wiegand input from external device such as ID card or user fingerprint.
  - 1:N identification : in 1:N mode, finger scan (authentication) is done with user's fingerprint only. As device sensor is always on input standby mode, 1:N scan starts right away once a finger is placed on.
  - Both : Both 1:1 verification and 1:N identification are supported.

- 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 or with BioStation, changing baud rate to lower value can be a solution.

- 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.

- 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**.

- Scan Timeout

  Scan Timeout specifies the 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.

- 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. Default value is **7**.

- 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. Default value is **0**.

- Matching Timeout

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

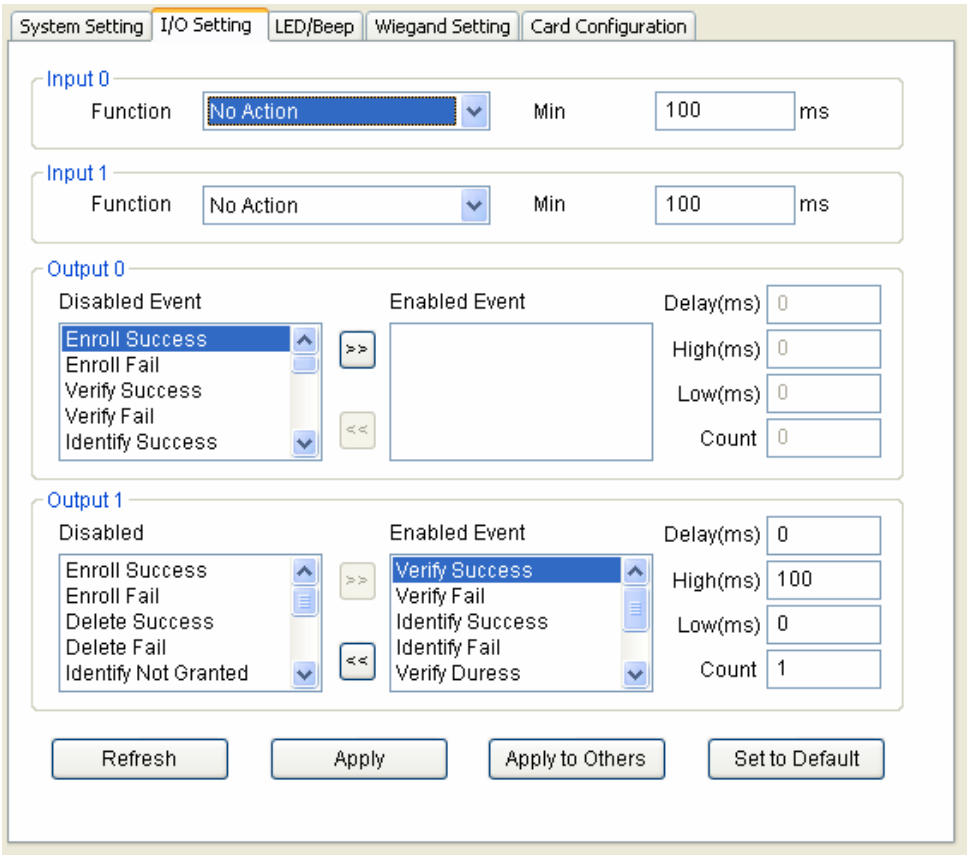
- Factory defaults of parameters

  BioEntry Factory defaults list of parameters for 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)

4.8.1. I/O Setting

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



- 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.

- 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

- Program sample for input port
  - If administrator wants to connect the wiegand input of the user ID to the input button to initialize enrollment, the following procedure is required.
  - Suppose to use input port 0, user should press a button for at least 500 ms to activate a function.
  - First, choose applicable device on device list window.
  - Choose a function of input port 0 with Enroll by Wiegand ID.
  - Input 500 as minimum input time of input port 0.
  - Press apply button to transfer new settings to applicable device.

- 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.

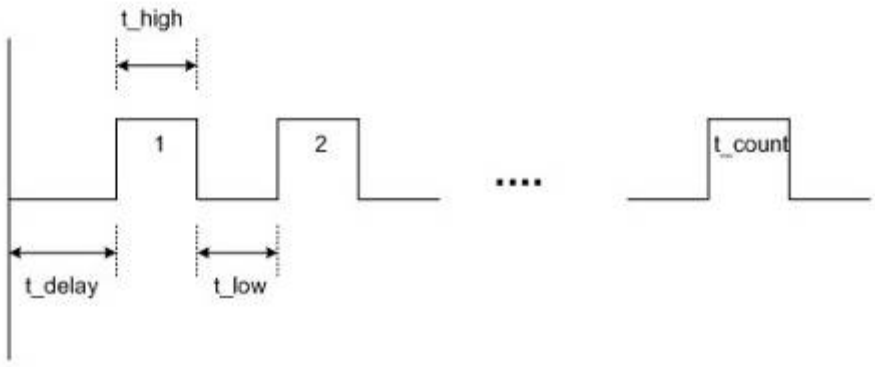
- Output events

Event	Description (when to activate the output port)
Enroll Success	When a user is successfully enrolled on the device
Enroll Fail	When enrollment fails
Identify Success	When identification is successfully done
Identify Fail	When the device 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 device is enabled implying device 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

- 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

- 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 device sends blinking output during 5 seconds.
  - When temper switch is on, the device sends steady output during 10 seconds.
  - Programming procedure is as follows:
  - First, select a target device 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:

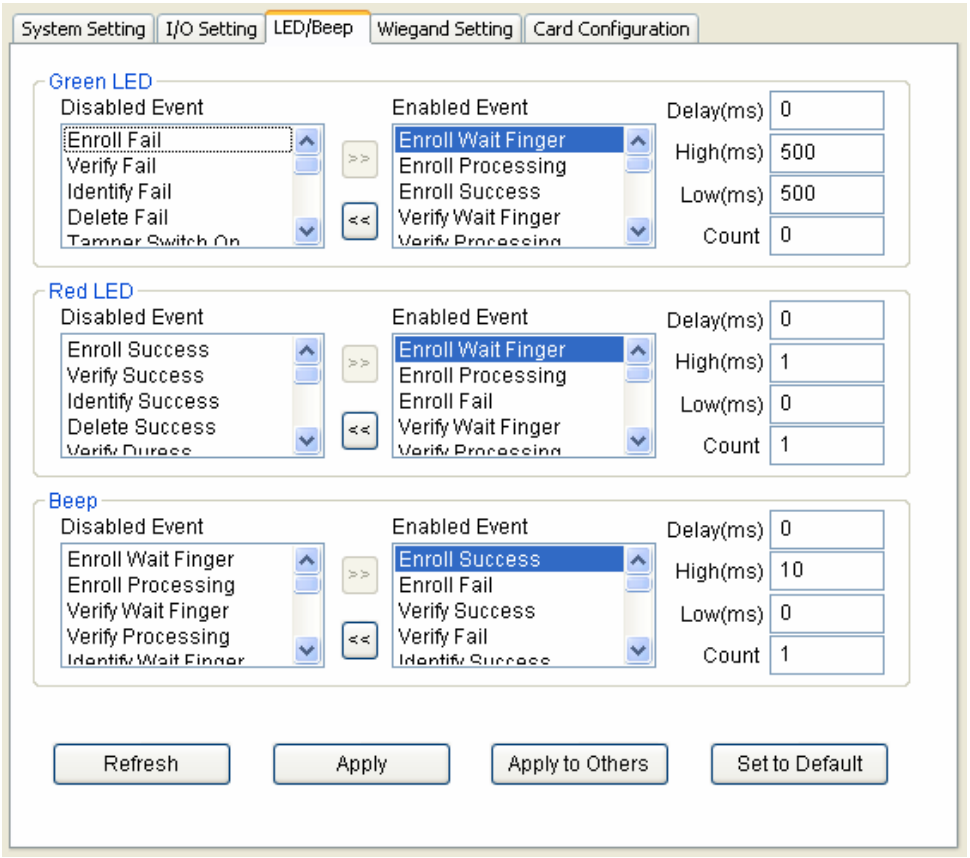
Event to be enabled	Output pattern parameters
Verify Duress	Delay : 0 High : 500 Low : 500 Count : 5
Identify Duress	Delay : 0 High : 500 Low : 500

	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 device.

4.8.2. LED/Beep sound Setting

There are two LED's and one beep on BioEntry device to provide processing status and result to users. The colors of two LED's are mixed to generate 3 colors, green, red, and amber. By selecting the LED/Beep Setting tab, the LED/Beep configuration page is updated on the main window.



- Configuration of LED/Beep

  Programming steps for LED and Beep is similar to output port configuration. Additional events are selectable, listed as

Event	Description (when to activate the output port)
Enroll Wait Finger	When the device is waiting for a finger scan to enroll
Enroll Processing	When the device is in enrollment process
Identify Wait Finger	When the device is waiting for a finger scan to identify
Identify Processing	When the device is in identification process
Verify Wait Finger	When the device is waiting for a finger scan to verify
Verify Processing	When the device is in verification process
Delete Wait Finger	When the device is waiting for a finger scan to delete

- Description of default LED/Beep configuration

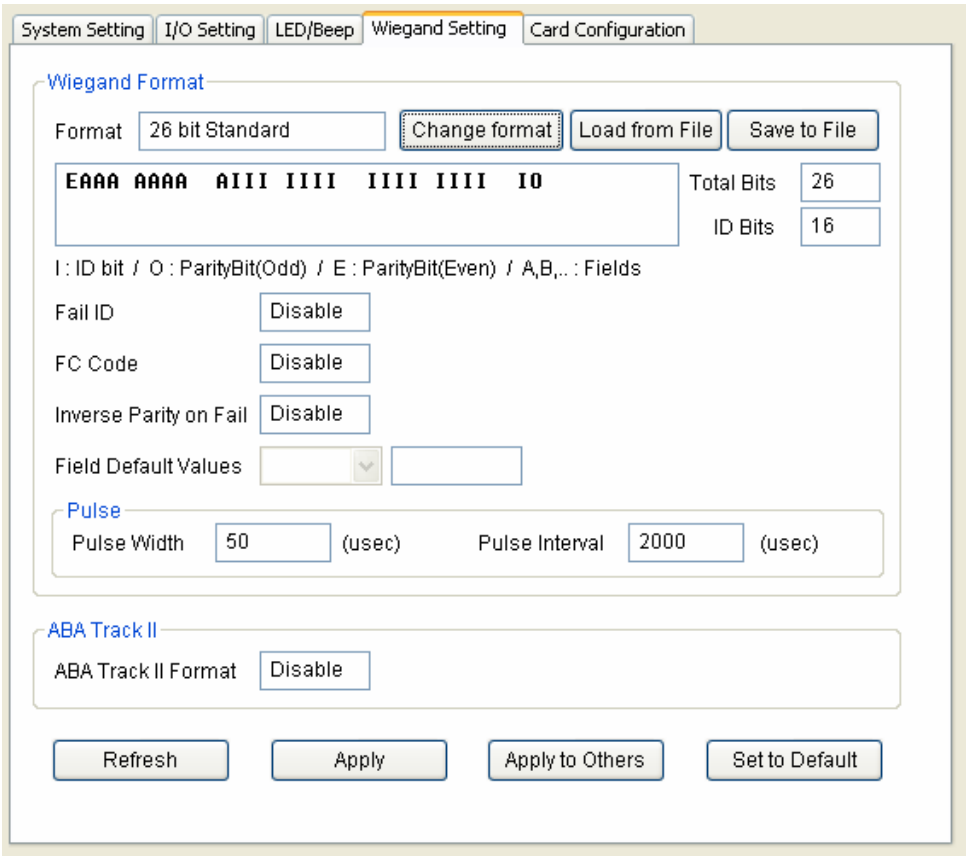
  By factory default, various output patterns are defined for LED and beep to show current status and processing result. The description of default LED/Beep configuration is listed as follows:

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	Steady red	Three short beep sounds

Delete Fail Command Card Fail		
Waiting Smart Card Input	Fast blinking red (fixed)	None

4.8.3. 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.



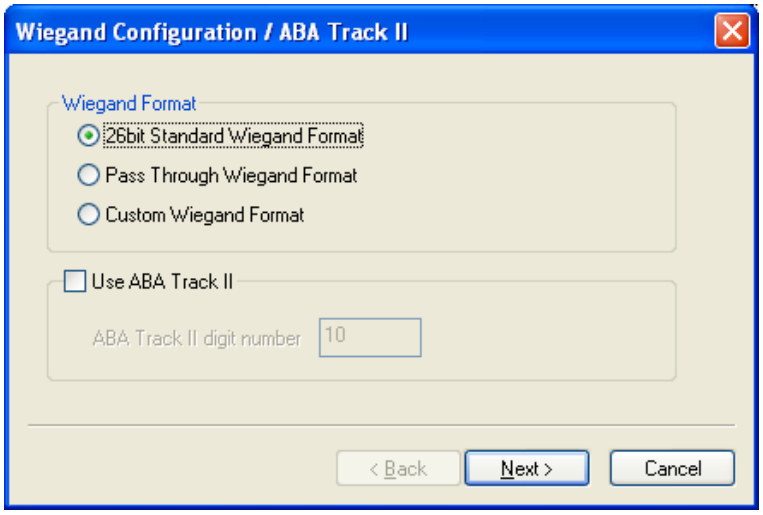
- Wiegand Format

  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 device 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

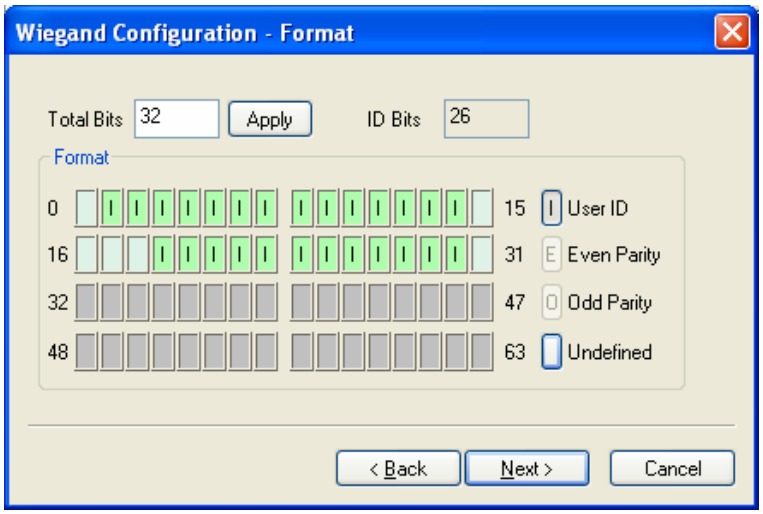
  Pass Through format is used when only the format of ID field is known. When the Wiegand input string is detected, BioEntry device extracts ID bits and starts verification with the ID. If the verification succeeds, the device outputs the Wiegand input string as unchanged. Parity check and advanced options 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.

▪ 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 device checks the parity bits first. If all the parity bits are correct, the device 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 device 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 IIIO

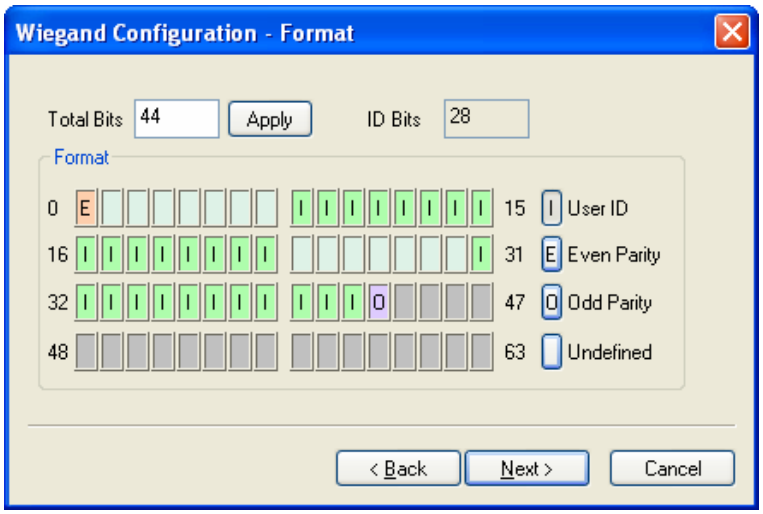
(left most bit is 0th bit, BIT0)

E: Even parity for BIT1 ~ BIT22

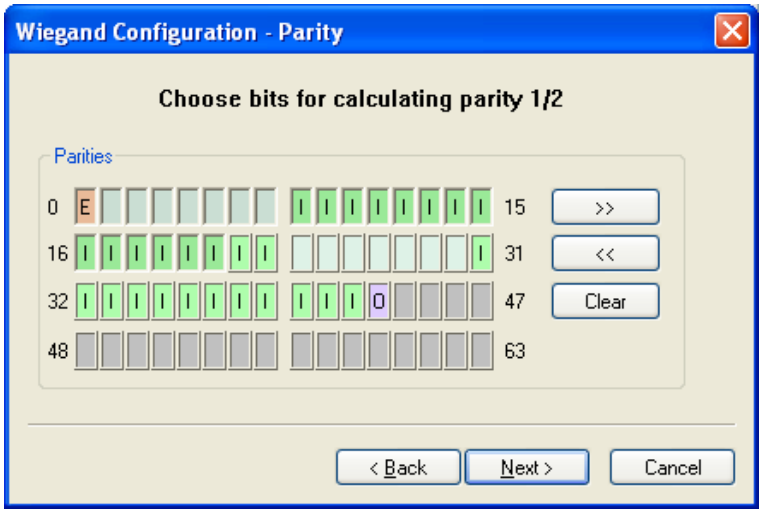
O: Odd parity for BIT23 ~ BIT42

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

You can configure this format in the following sequences.



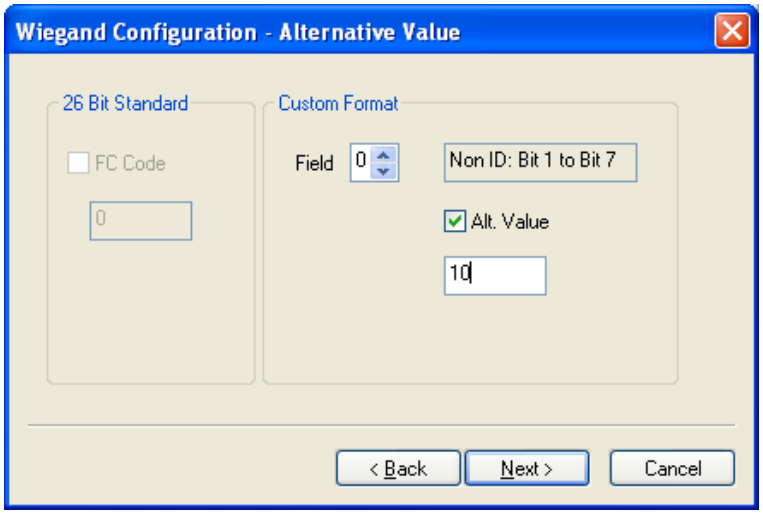
- Enter 44 in the **Total Bits** field.
- Select **Even Parity**.
- Press the even parity bit. In this example, it is BIT0.
- Select Odd Parity and press the odd parity bit and User ID according to the definition.
- Press **Next**.



- Press the bits which are used in calculating the first parity bit. In this example, they are BIT1 ~ BIT22
- Press >>.
- Press the bits which are used in calculating the second parity bit. In this example, they are BIT23~ BIT42.
- Press **Next**.

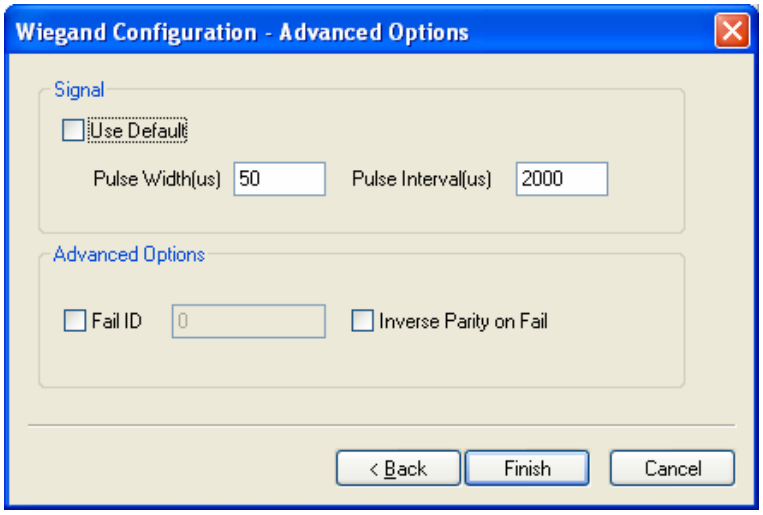
- Alternative values

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



- 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.



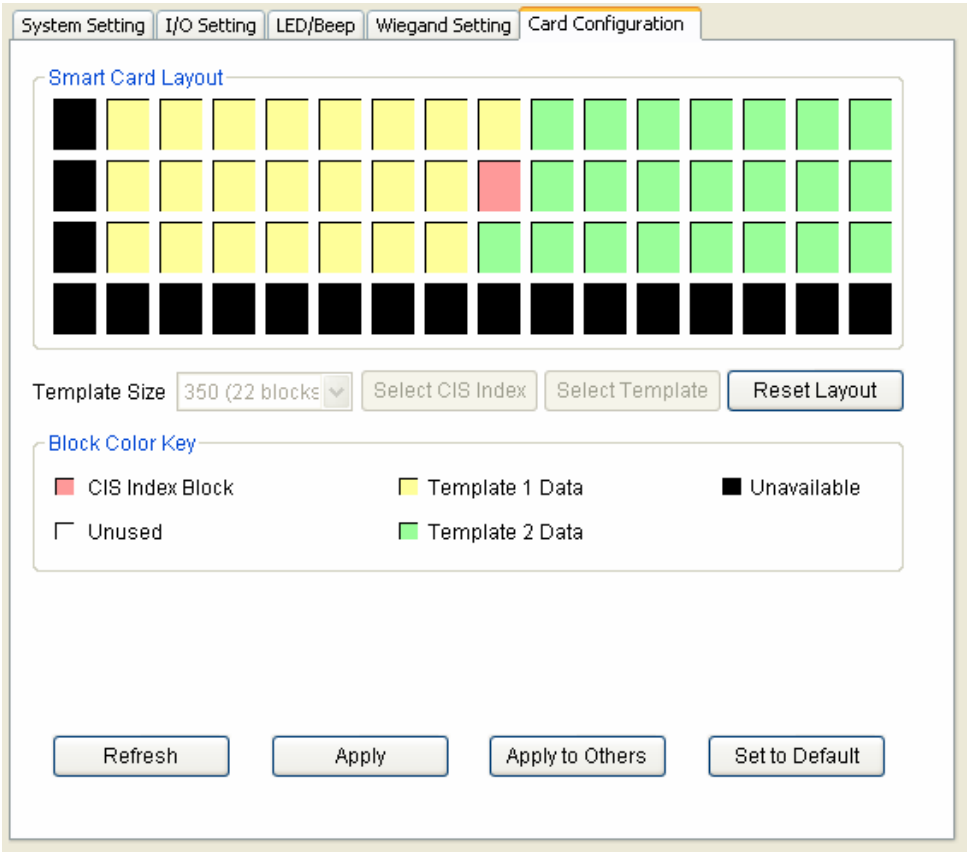
  - Use Default: Uses default values for Wiegand signals.

- **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.

4.8.4. Smart Card setting

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.

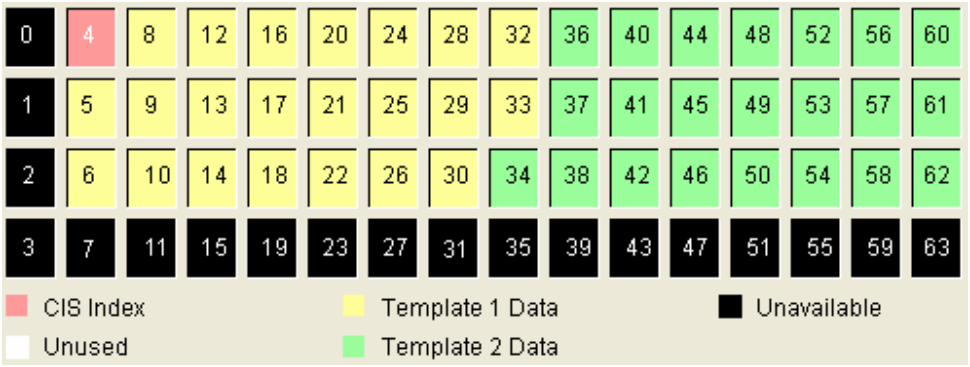
Note : ***It is recommended that only advanced users attempt to change the layout since improper changes may render the smart card unusable. Read this chapter carefully for changing the layout from the default configuration.***



- 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.
- Editing procedure

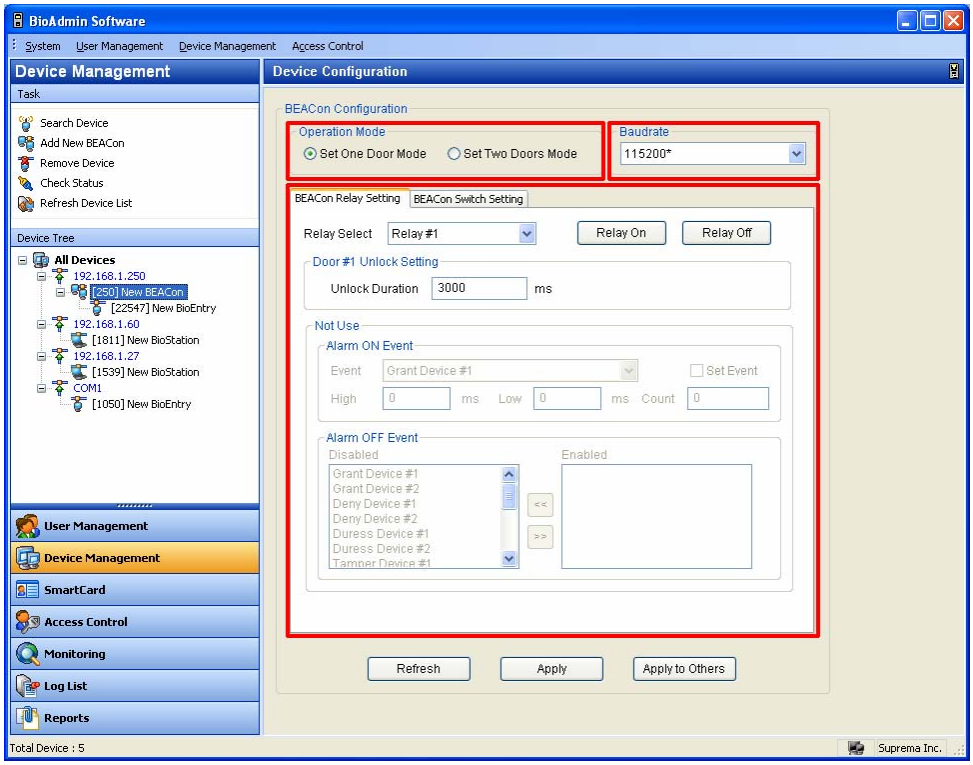
  To configure customer's layout, following procedures are required.
  - Initialize all the blocks to unused ones by pressing the Reset Layout button.
  - Select the required template size.
  - Press the Select CIS Index button and click an unused block to select a CIS index block.
  - Press the Select 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 devices.
- Factory default layout

  Factory default smart card layout is as follows :



4.9. 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 transfer 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 menu is divided by separate tabs, such as BEACon Relay Setting and BEACon Switch Setting. For the detailed operation of BEACon, refer to BEACon operation manual.

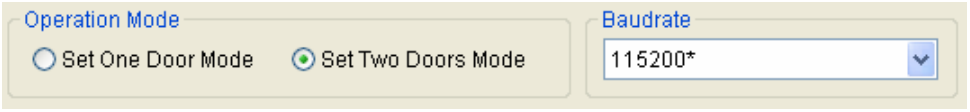
4.9.1. Operation Mode

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.

4.9.2. Signaling speed (Baud rate)

The Baud rate window shows the transfer speed of the selected BEACon.

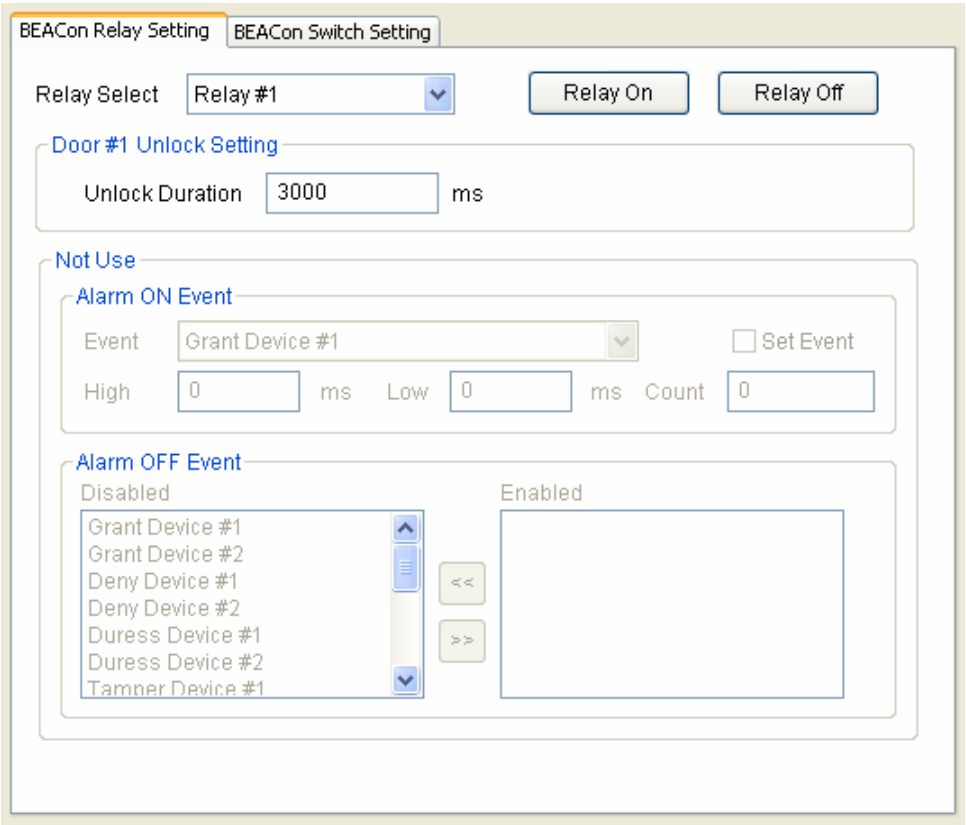
- Baud rate: On this menu, you can select the transfer speed of BEACon. If you change the Baud rate on this menu, communication speed between BEACon and host PC will be changed.
- Once you change the Baud rate of BEACon, you also need to accord the Baud rate of BioEntry and BioStation with the changed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



4.9.3. 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.

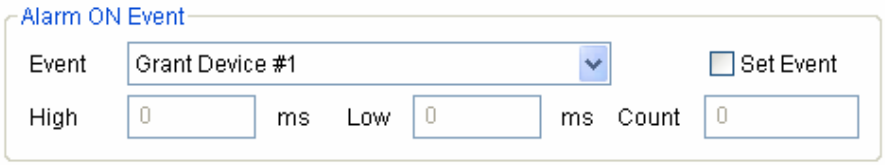
- Select a relay to set up the configuration. Once you select a relay, applicable items for the selected relay will be activated on the relay setting window.
- You can also open/close the relays by pressing the **Relay On / Relay Off** buttons.

- Unlock Setting

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

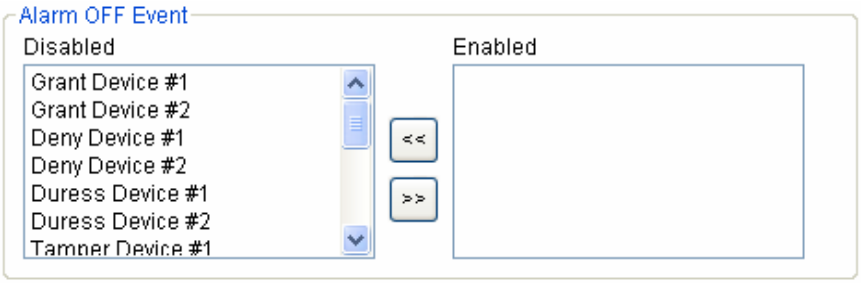
- Alarm On Event:

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:

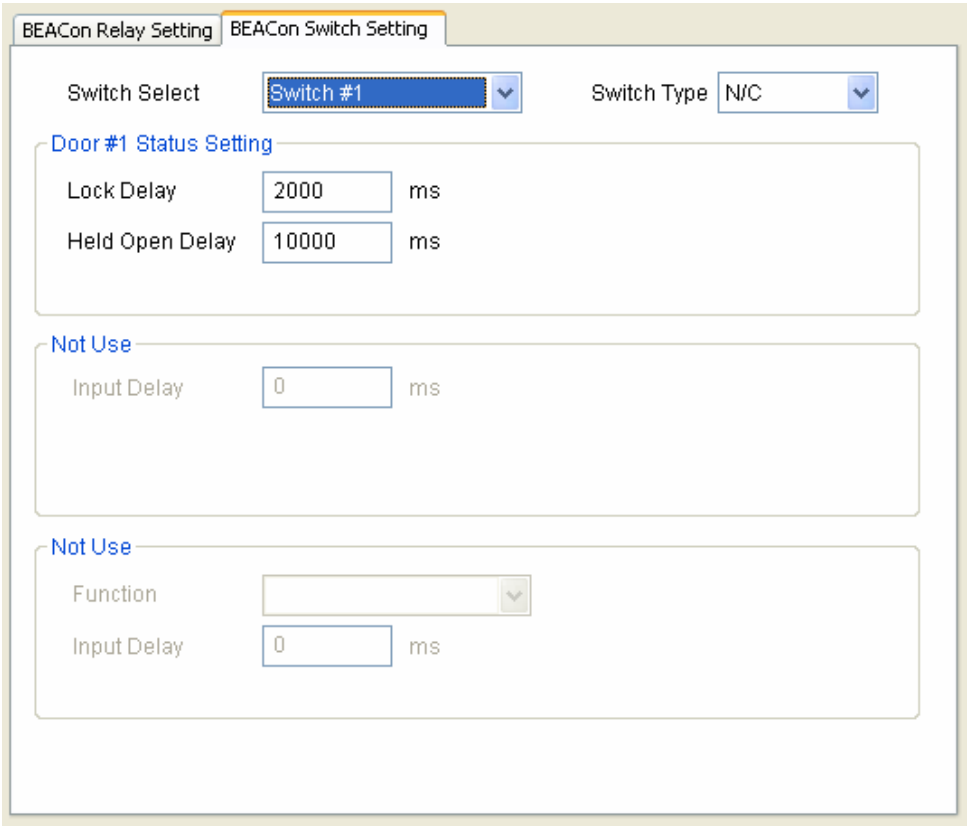
  Select alarm off events. You can enable the alarm off events simply by double clicking the events on the disabled event list. If any of the alarm off events is triggered, the alarm will be deactivated, regardless of remaining duration or pulse counts.



4.9.4. 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.



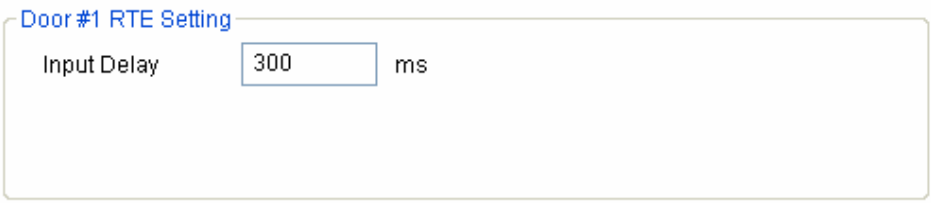
- Select a switch to set up the configuration. Once you select a switch, applicable items for the selected switch will be activated on the switch setting window.

- 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 held open door event will be triggered.

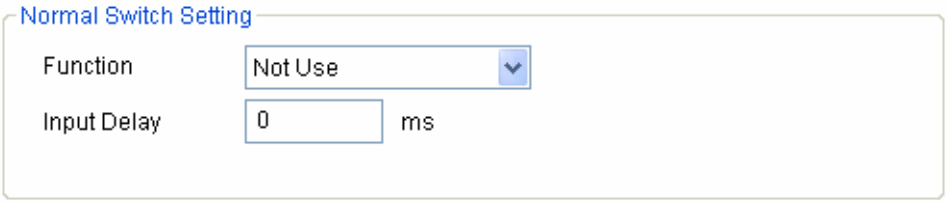
- Door RTE Setting

  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.



4.9.5. Refresh / Apply / Transfer (apply to another device)

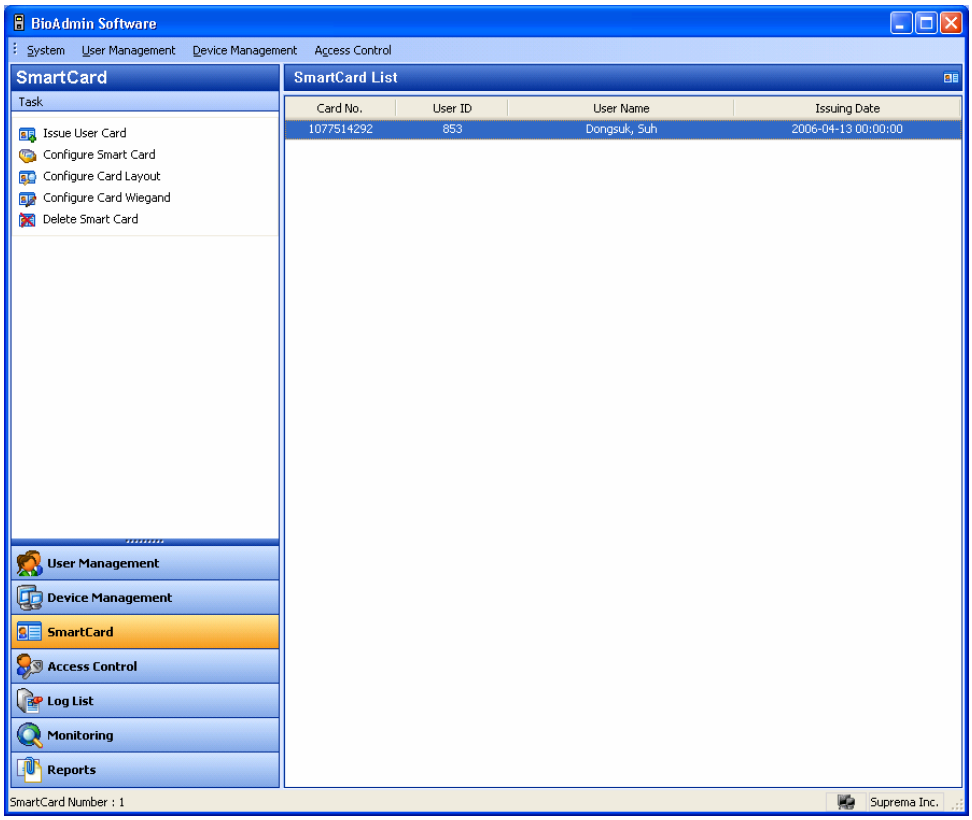
- Refresh : You can restore the original configuration by pressing the **Refresh** button before pressing Apply button.
- Apply : After changing the configuration, you need to press the **Apply** button to save.
- Transfer : You can transmit the changed configurations to other devices by pressing the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

5. Smartcard

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



5.1. Configuration 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.

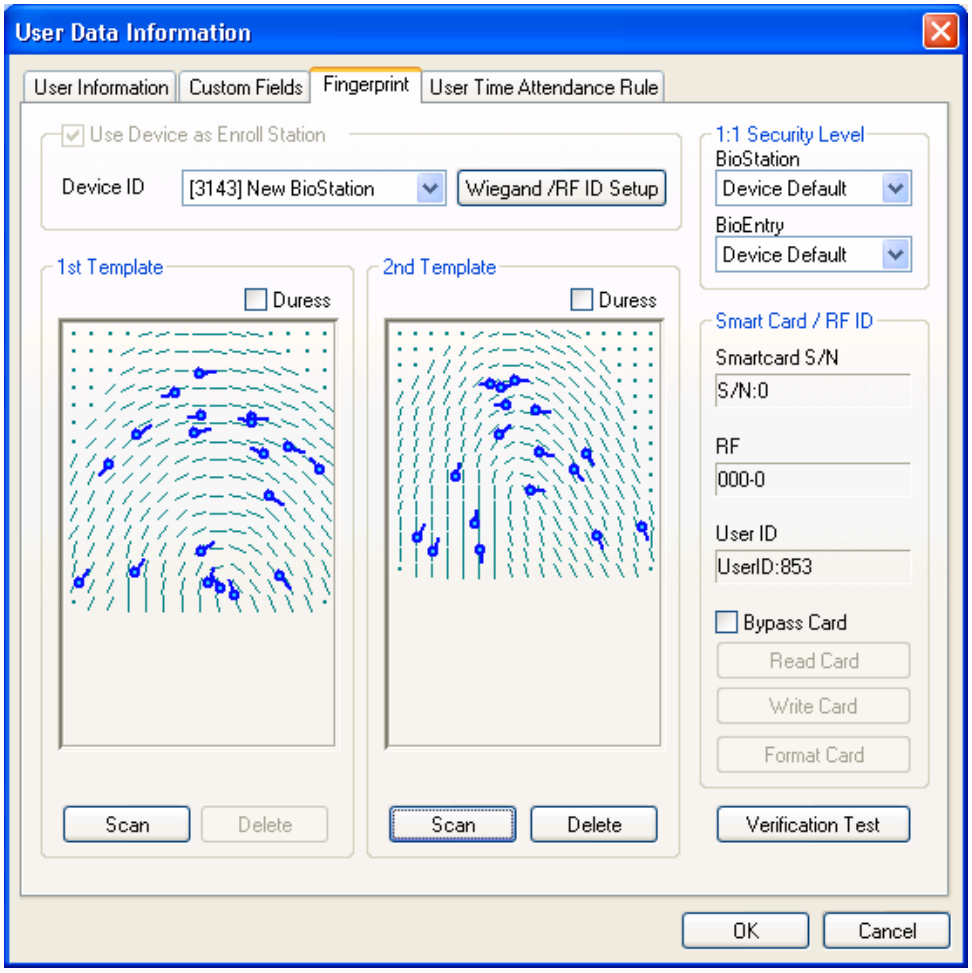
5.2. Smartcard List

The Smartcard list includes the following information of the Smartcards.

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

5.3. Card issue

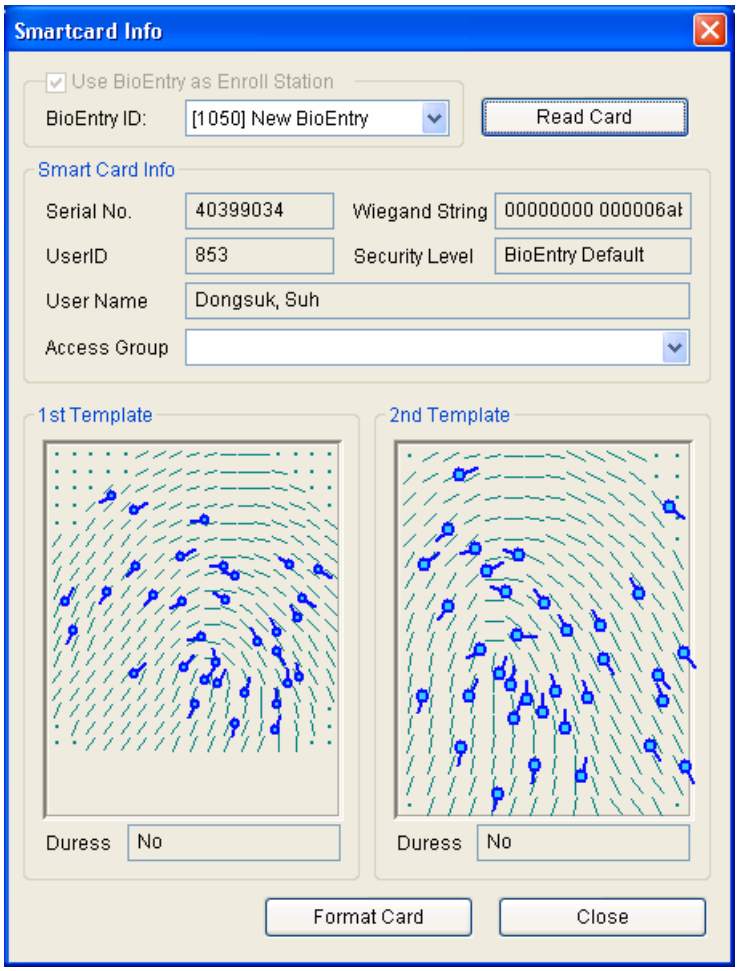
The **Issue User Card** menu enables a pop-up window to issue a user's smart card. For the detailed operation, refer to the issuing procedure on the User Management menu.



5.4. 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 Device/Writer, you can also read the smart card information directly through BioEntry by check on **Use BioEntry as Enroll Station.**



5.4.1. Read 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 3. User Management.

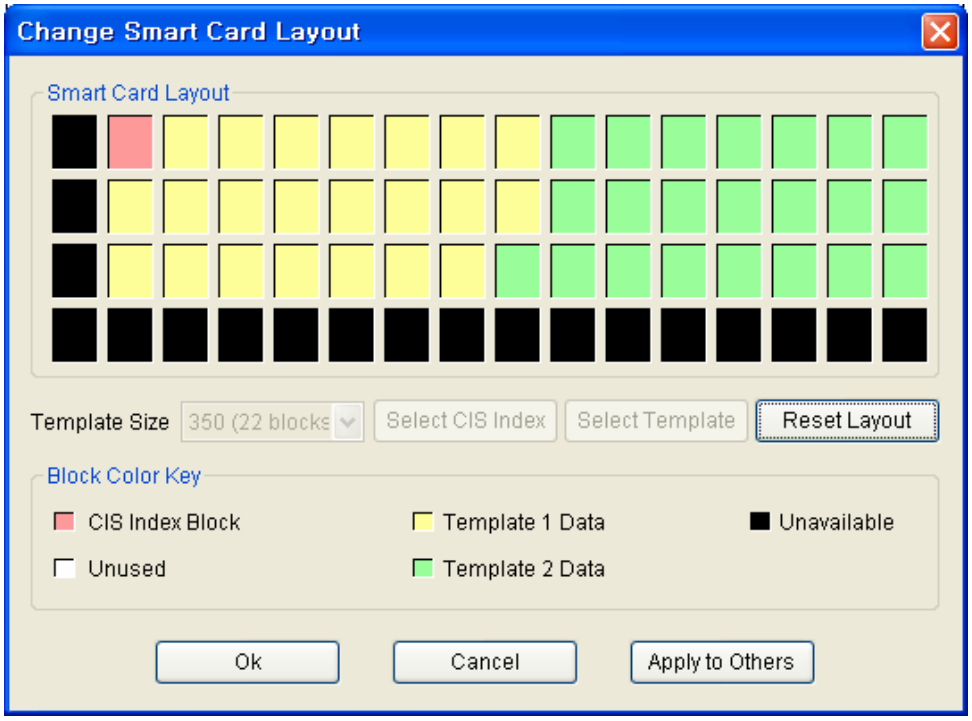
5.4.2. Smart card format

On this Manage Smartcard window, the formatting can be processed similarly to the formatting process described in Chapter 3. User Management.

5.5. Edit 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 Layout** 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.



5.5.1. Configuration of smartcard layout edit page

The Configure Smartcard layout page is divided into 3 sectors :

- Smart Card Layout

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

- Smart Card Layout

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

- New configuration

  This sector is used for editing new layout to be applied to the devices 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 device. **Transfer**

button transmits new layout to the selected BioEntry™ device, selected group, or all BioEntry™ devices. Several control buttons for editing layout also exist.

5.5.2. Size of Fingerprint data (Template)

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

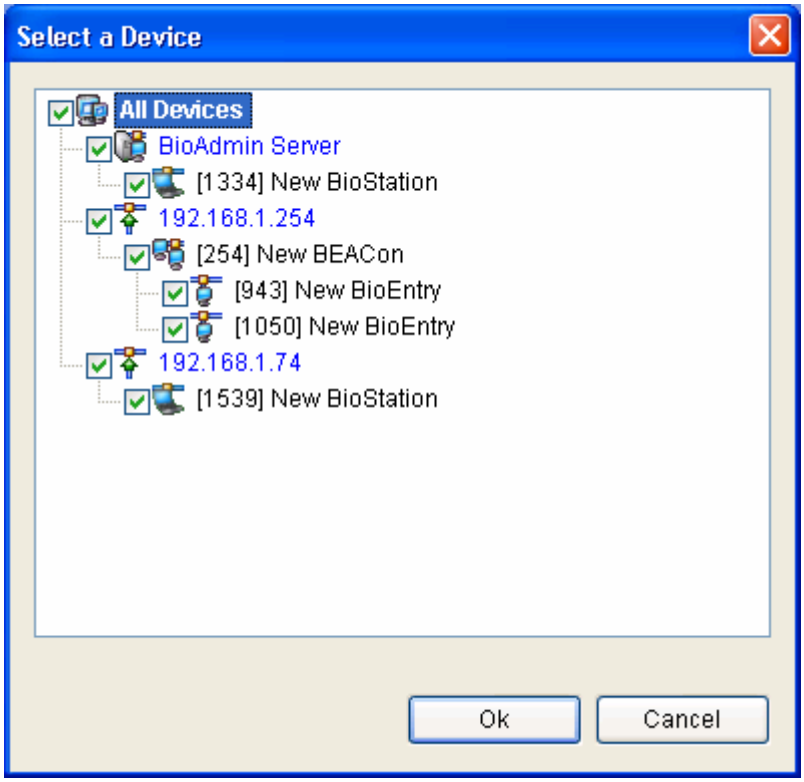
5.5.3. Block

- 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.

5.5.4. Editing process

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

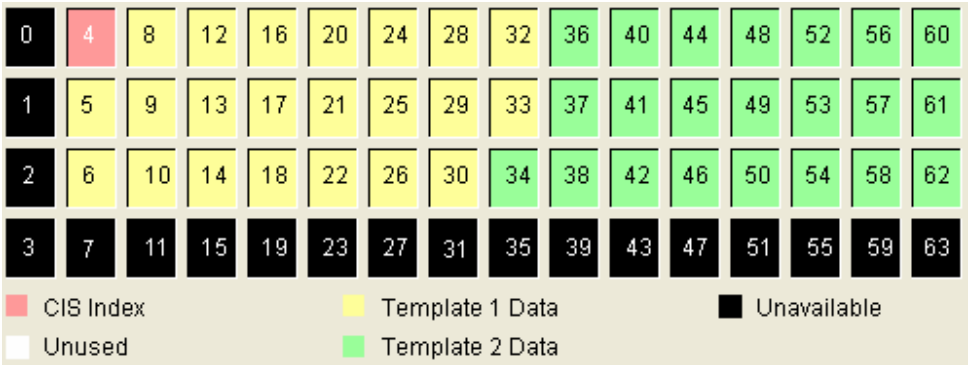
- Initialize all the blocks to unused ones by pressing the **Reset Layout** button.
- Select the required template size.
- Press the **Select CIS Index** button and click an unused block to select a CIS index block.
- Press the **Select Template** button and click an unused block to indicate the start 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 devices.



- 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 device/writer.
- The saved layout is also applied in issuing a new smartcard using PC USB smartcard device/writer.

5.5.5. Factory default (initial setting) layout

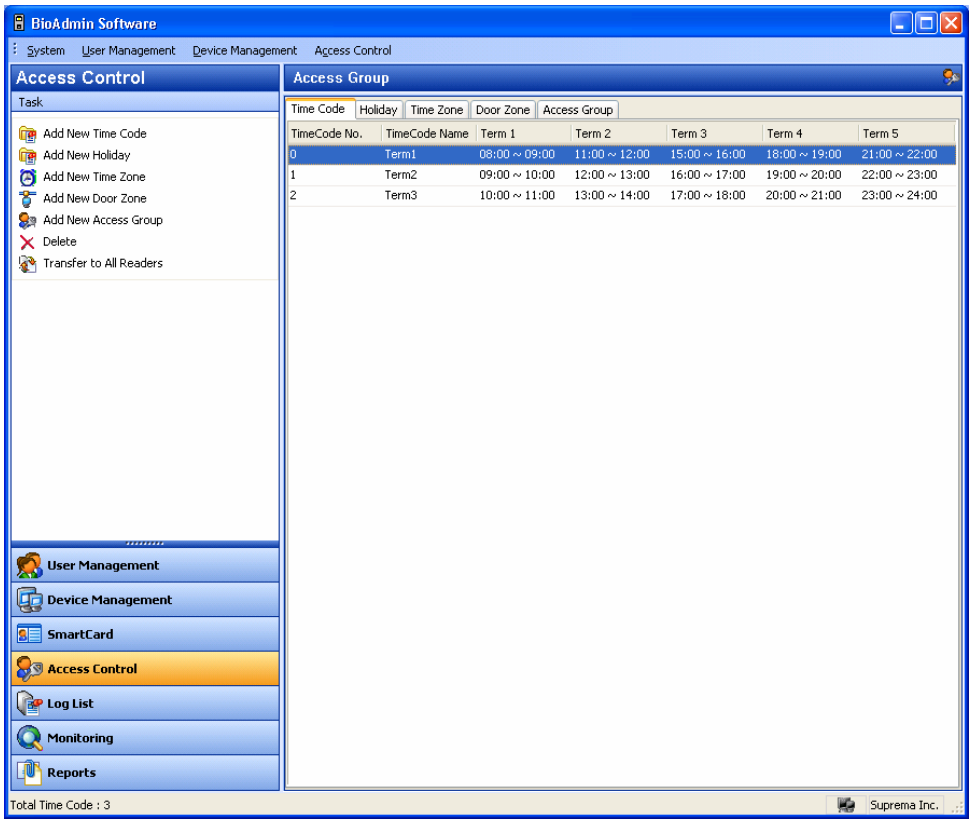
Factory default smart card layout is as follows :



6. Access (In/Out) 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™ device does not have the access group information, the user is allowed to enter the door without restriction.

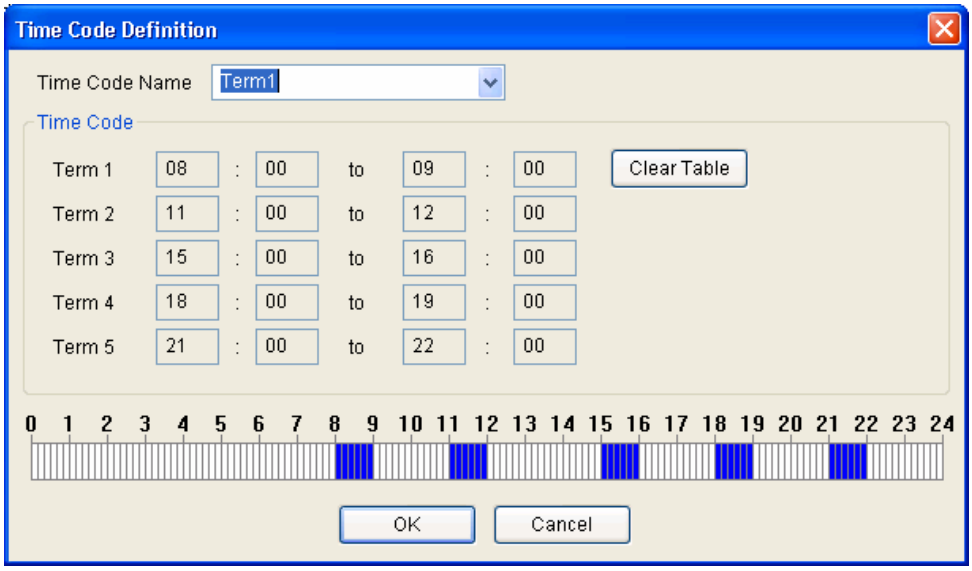


6.1. Time zone setting

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.



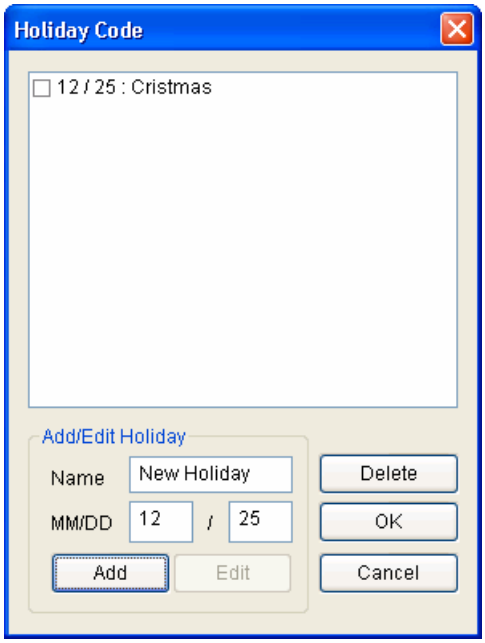
- Enter the name of time code.
- Set up the time code by entering time on the boxes.
- You can also set up the time code simply by dragging on the time bar on the bottom of time definition window.
- Press the **OK** button to add the time code on time code list.

6.2. Holiday setting

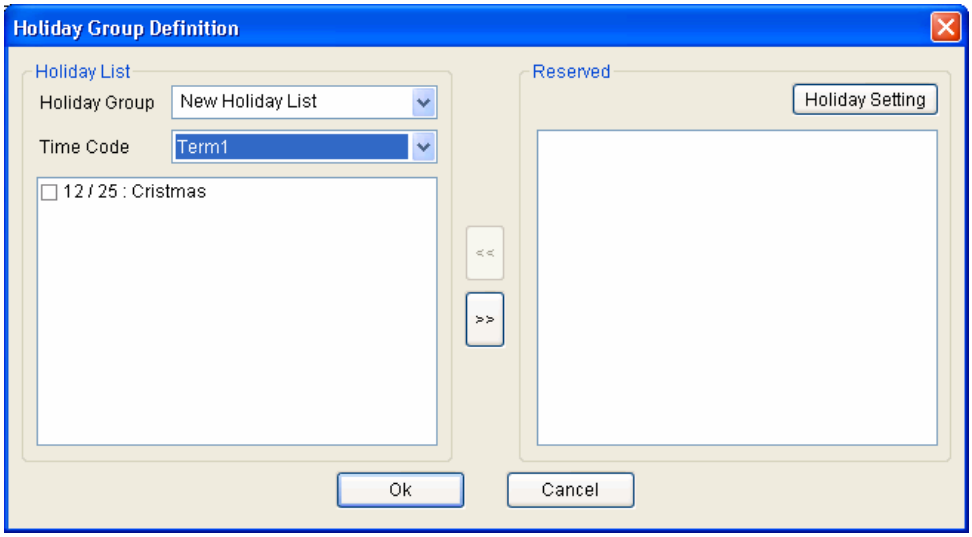
To include holidays on the Time Zone, you need to set up holidays in advance.

Detailed operations are 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.



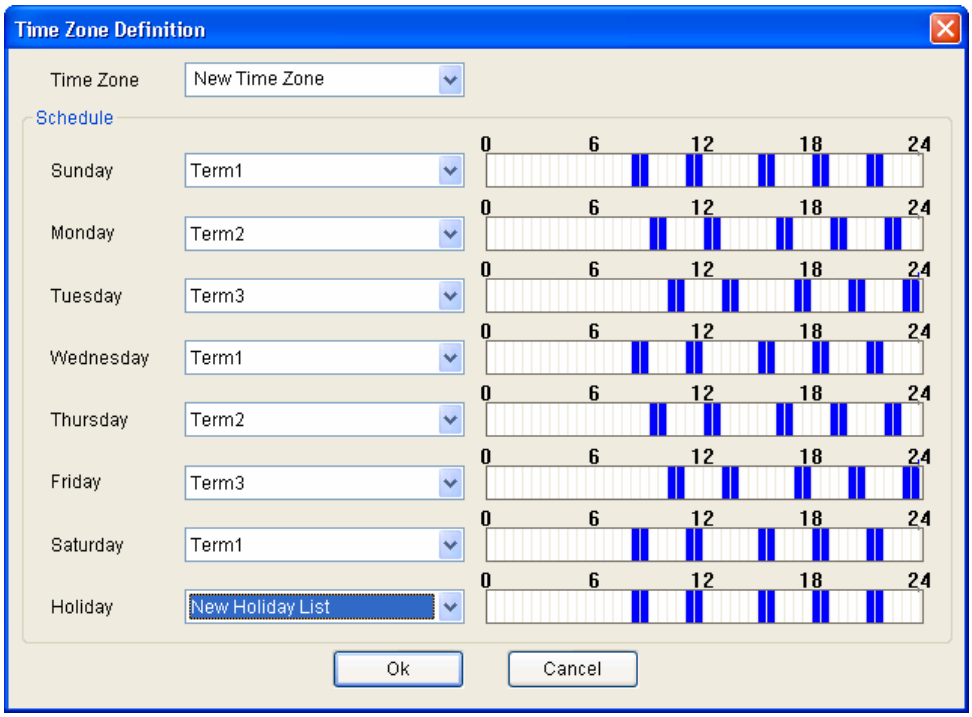
- Press **OK** button to add the holiday on the holiday list.

6.3. I/O time zone setting

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.

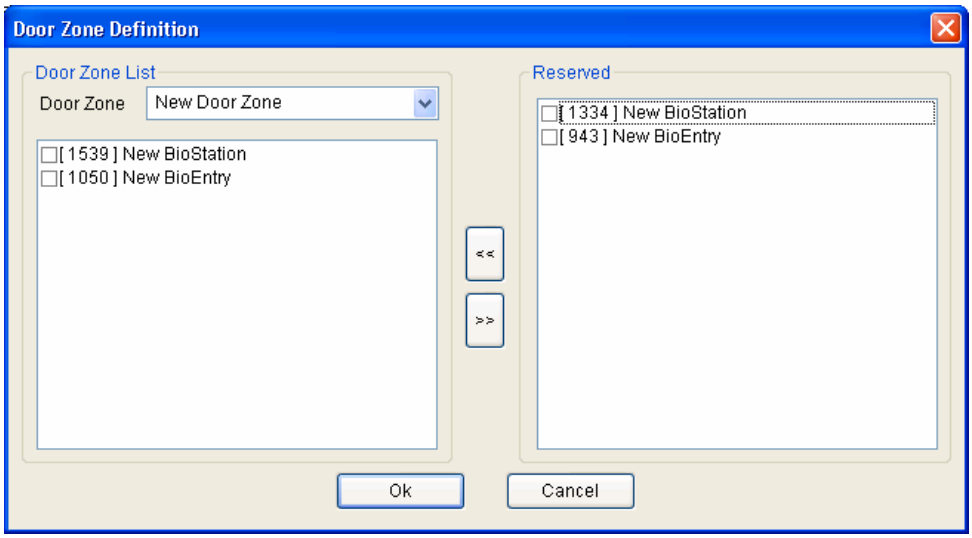


- Select a time code for each day from Monday to Sunday.
- Select a holyday group for the time zone.
- Press the **OK** button to add the holiday group to the time zone list.

6.4. I/O Door Zone setting

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

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

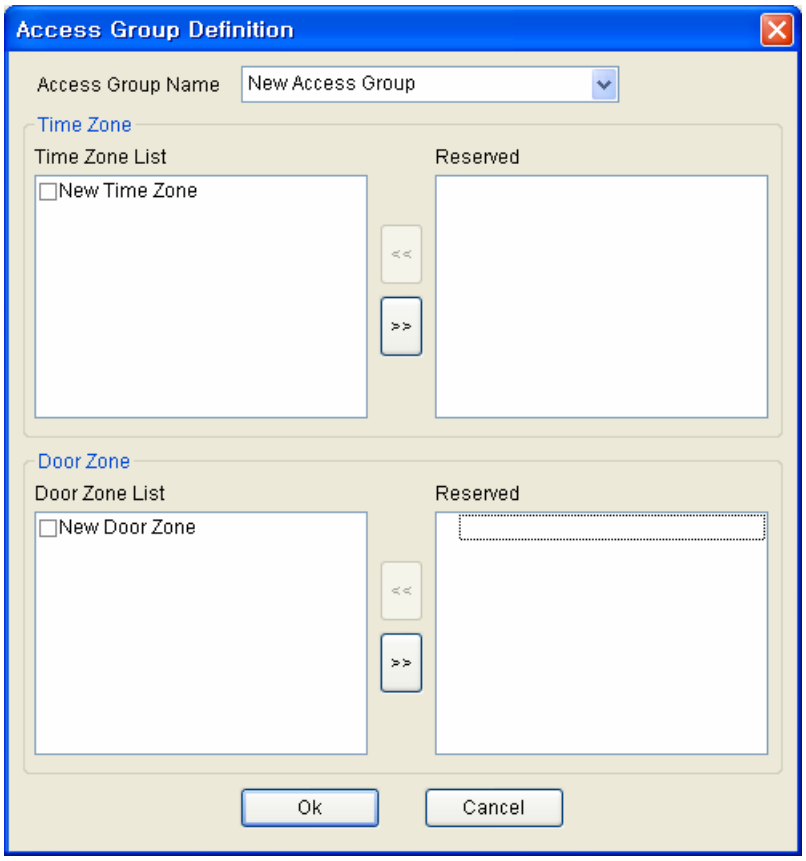


- Press the **OK** button to add the door zone on the door zone list.

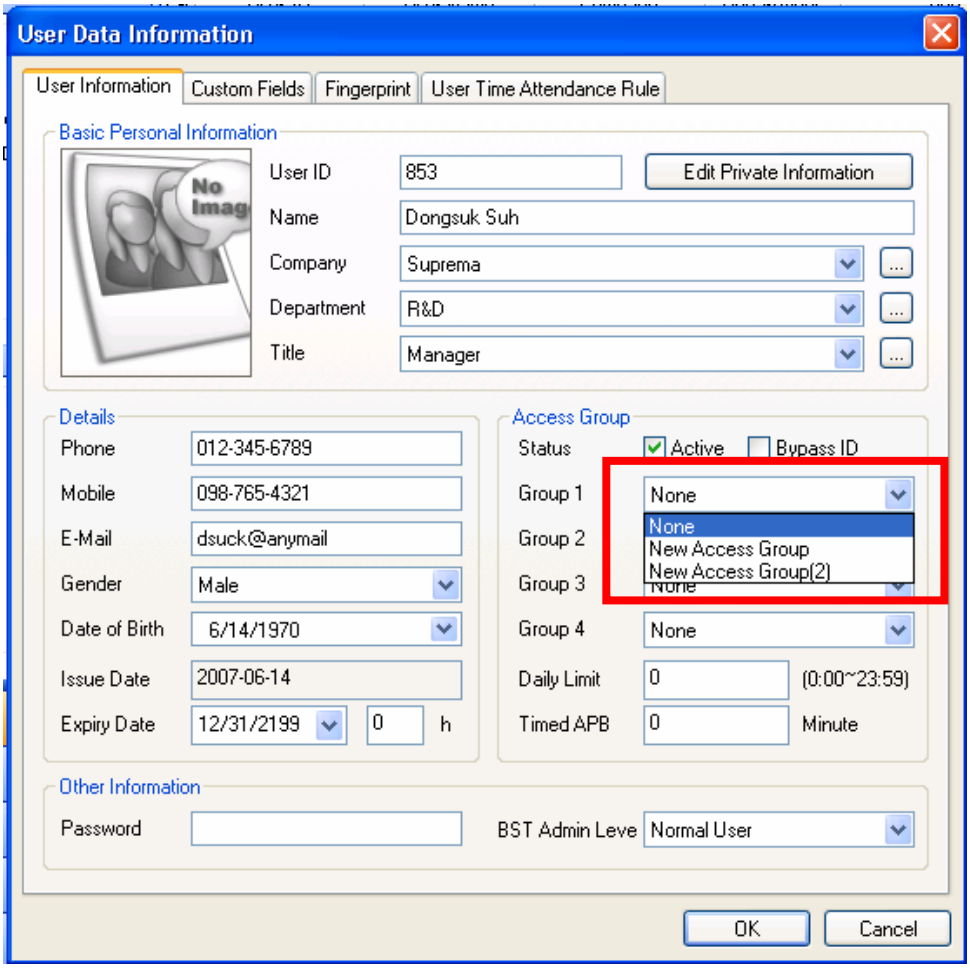
6.5. Access (I/O) Group setting

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.



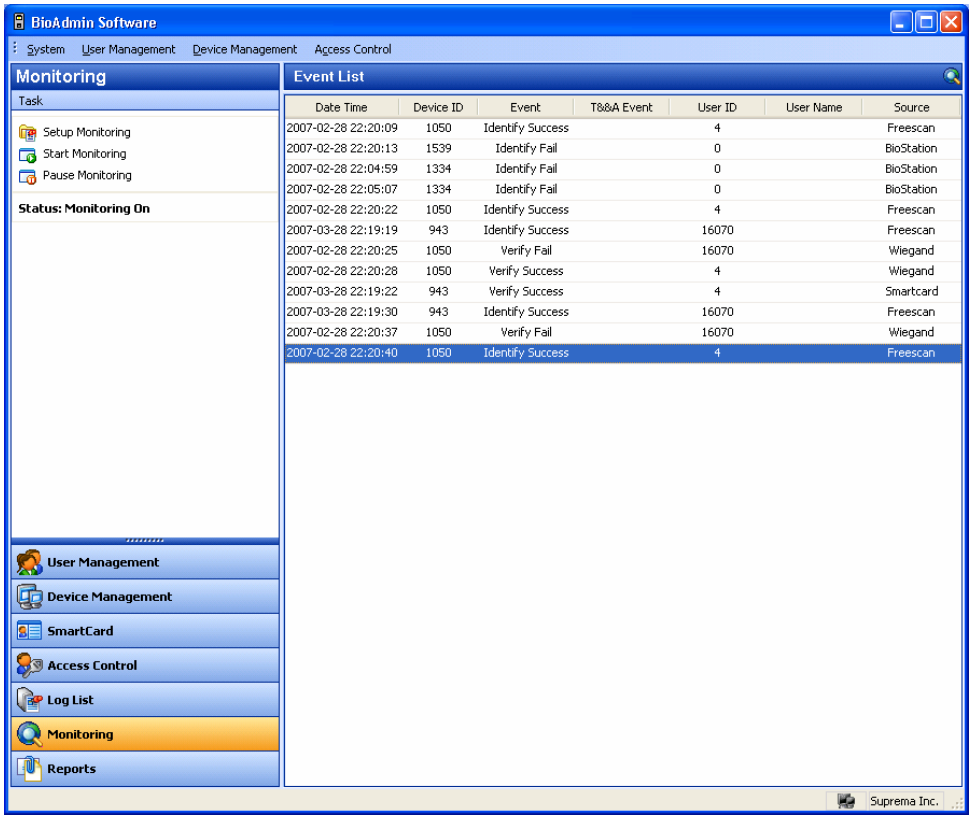
- Press the **OK** button to add the selected access group to the access group list. You can apply this access group to users on the **User Management** menu.



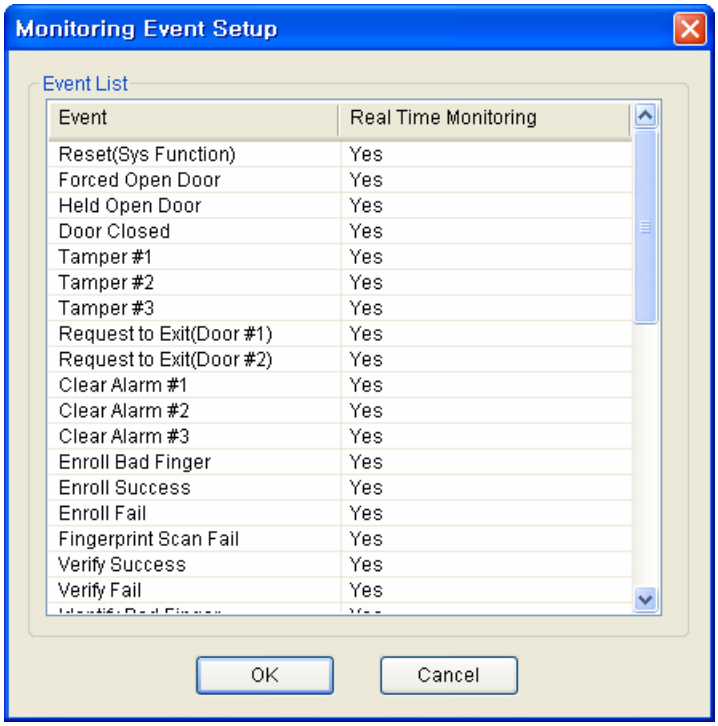
- For the detailed operation on User data, refer to Chapter 3. User Management menu.

7. Monitoring

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



7.1. Monitoring setup



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.

7.2. Start Monitoring

- By pressing the S**tart Monitoring** button, you can start the real time monitoring of the log events from all networked BioEntry and BioStation.
- 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 and BioStation.

> Monitoring is automatically started when the menu **Monitoring** is selected from another menu. So, the **Start Monitoring** is needed only to restart

monitoring after pausing monitoring.

7.3. Pause Monitoring

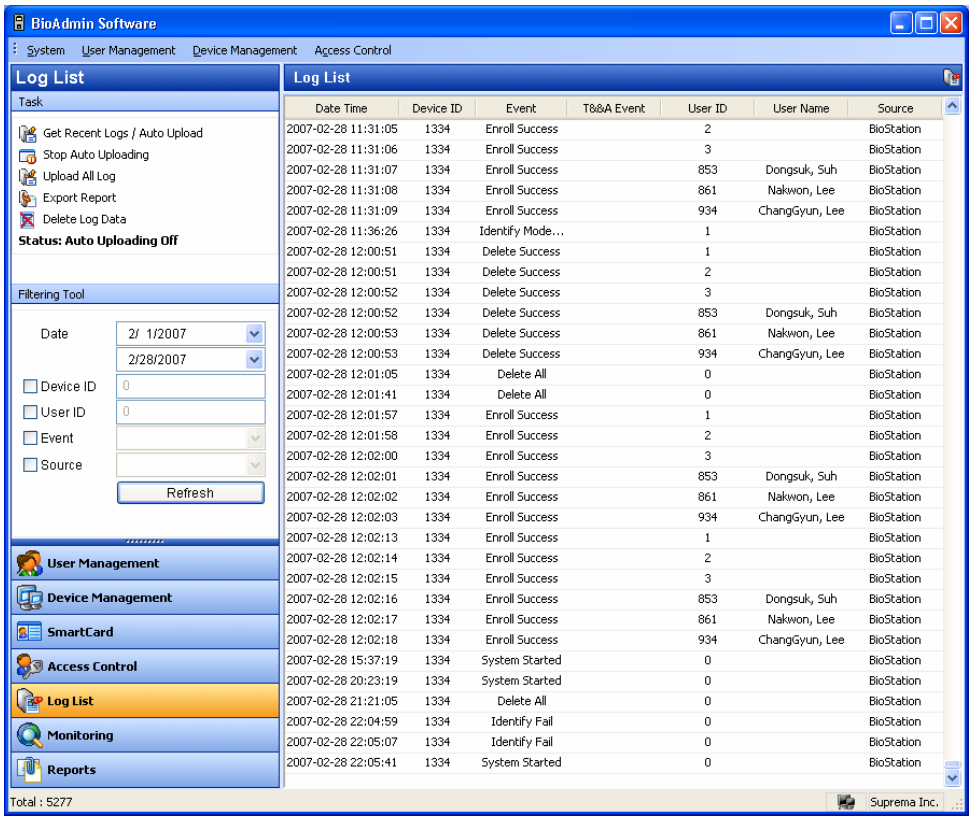
By pressing the **Pause Monitoring** menu, you can stop monitoring.

8. Log List

The Reports menu covers the following operations:

- Management of log database stored on host PC
- Upload new log events from BioEntry and BioStation into the log database

By selecting the Log List, the log list page is updated on the main window.



8.1. Configuration of Log check 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

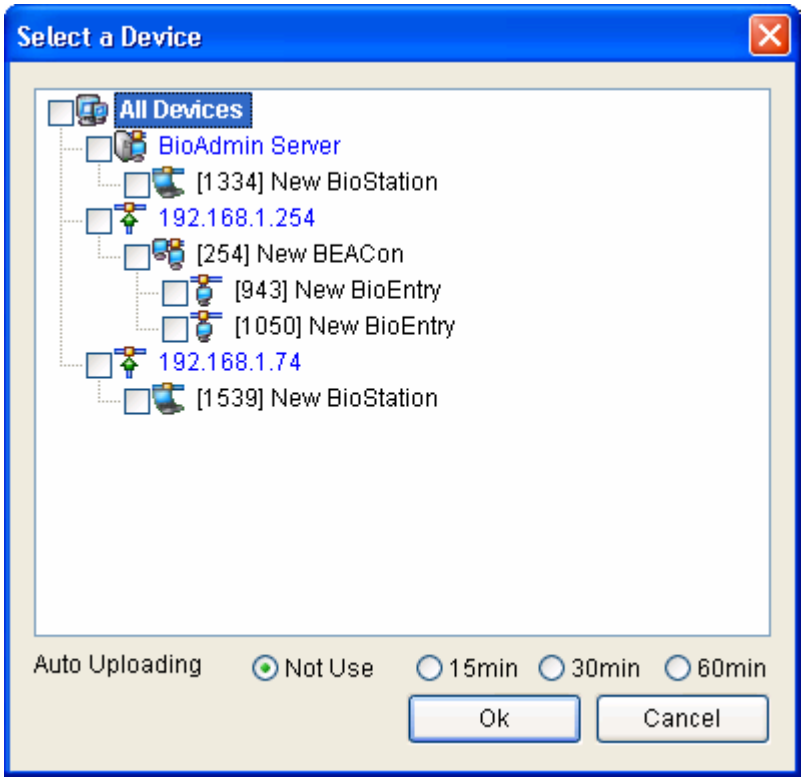
  Task box includes buttons to control basic operations of the Log List page.

8.2. Manage Log database

8.2.1. Get recent logs

In case of pressing **get recent logs/ auto upload** button, window for select device pops up and as to selected device here, log information newly generated after log information in BioAdmin is uploaded.

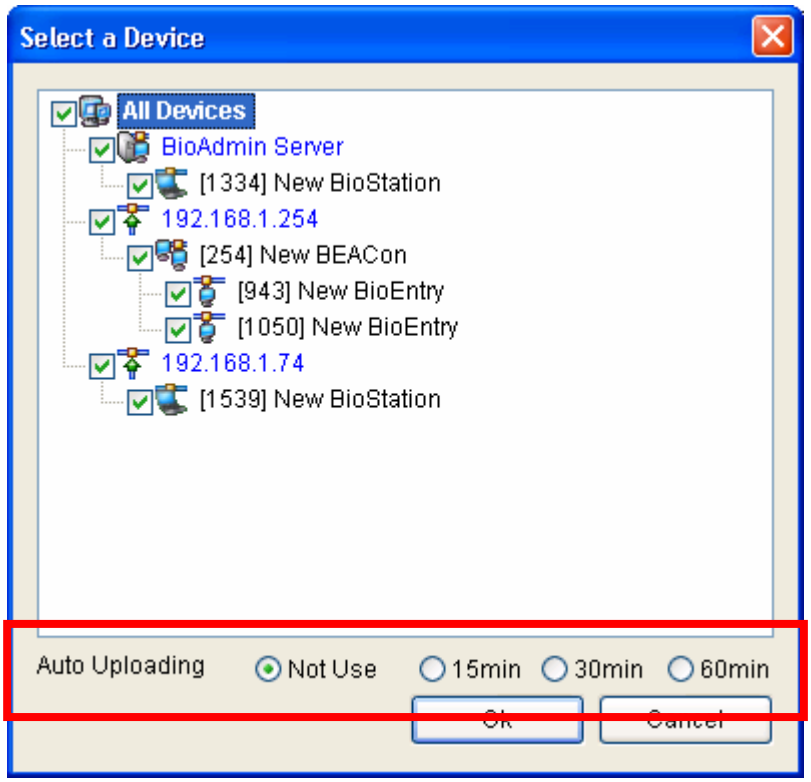
For the BioStation connected to BioAdmin Server, you do not need to get logs from them, because logs will be automatically saved on BioAdmin Server on real time.



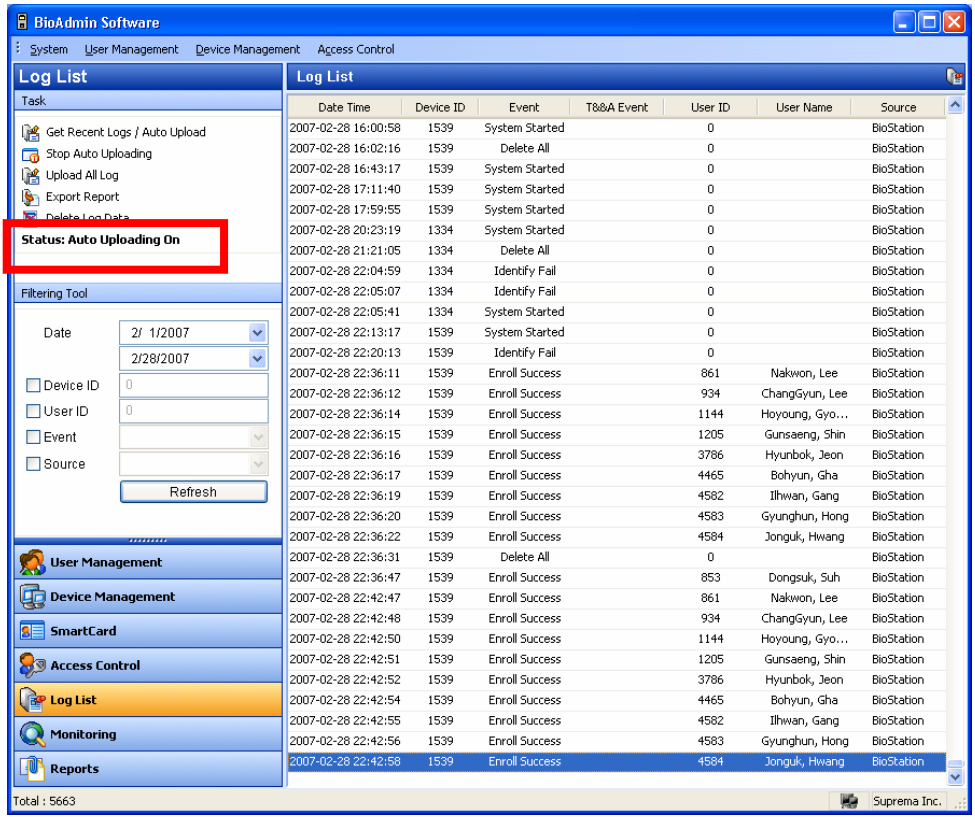
8.2.2. Auto uploading setting

In case of pressing **get recent logs/ auto upload** button, log information generated in BioEntry and BioStation for set period can be uploaded automatically to BioAdmin. Administrator can execute auto uploading by choosing 15 min / 30

min / 60 min according to applied environment.



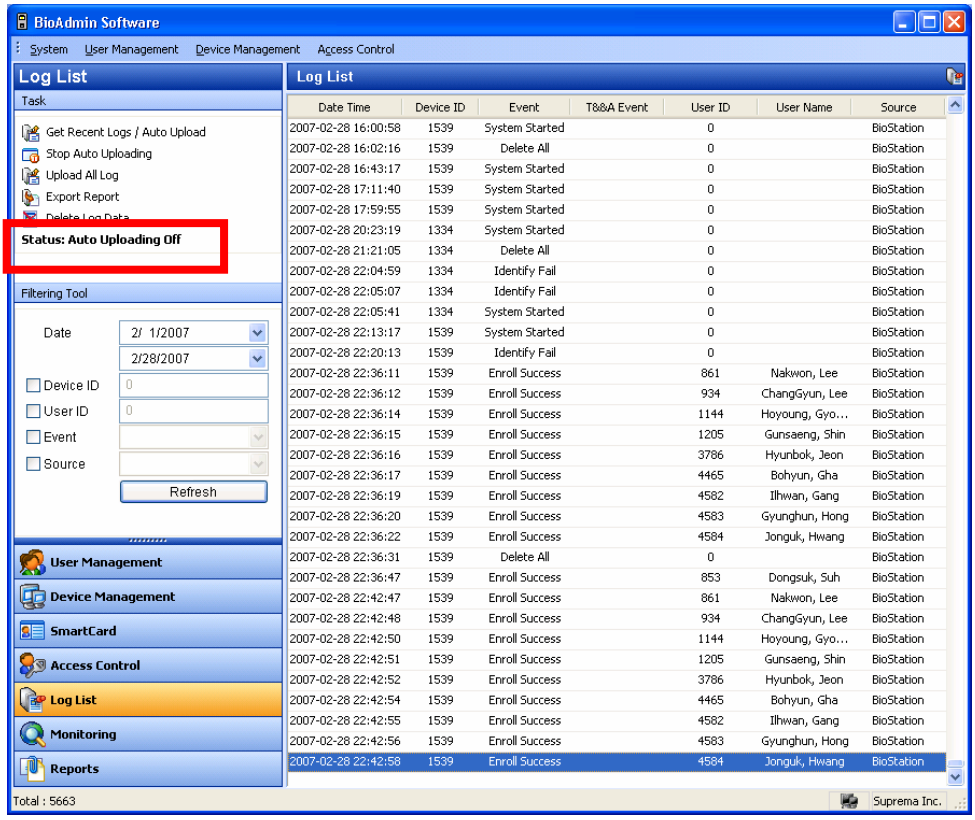
Once auto uploading is applied, **status : auto uploading on** is indicated on task box.



8.2.3. Release auto uploading

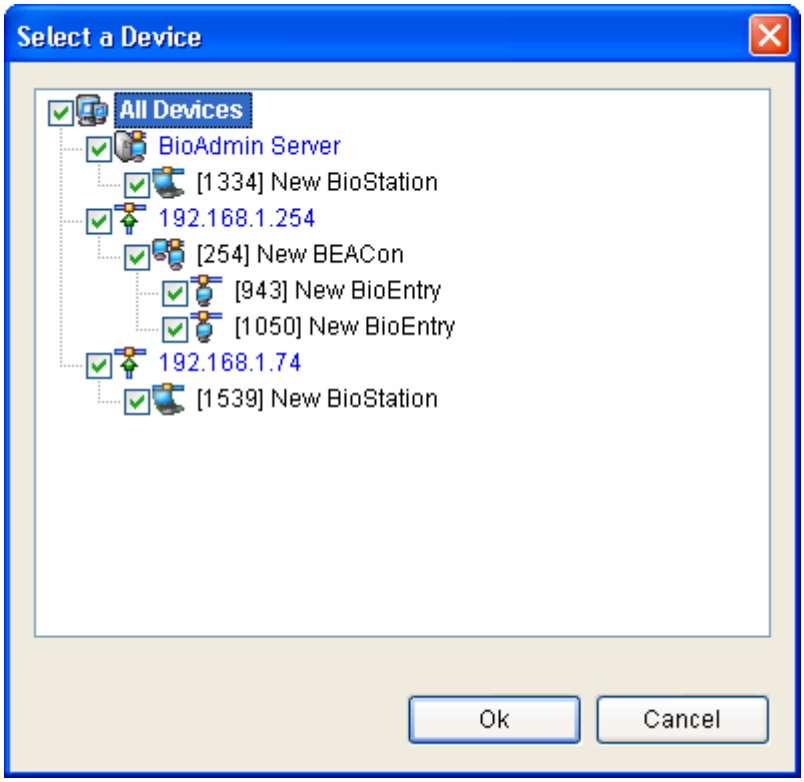
In case of pressing **stop auto uploading** button, user can release set auto uploading. Also, in case of disabled mode when setting time transfer, user can release time transfer.

Once auto uploading is released, **status : auto uploading off** is indicated on task box



8.2.4. Upload all logs

In case of pressing **upload all logs** button, select device window appears and all logs of device selected here are uploaded. In case partial log information remains in BioAdmin, existing log information is kept as it is and new log information is uploaded.

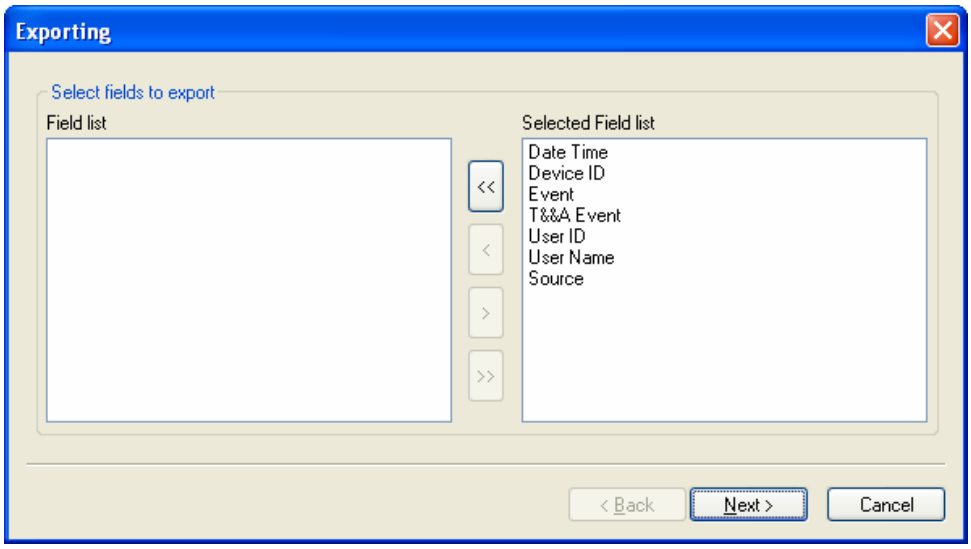


8.2.5. Export Report

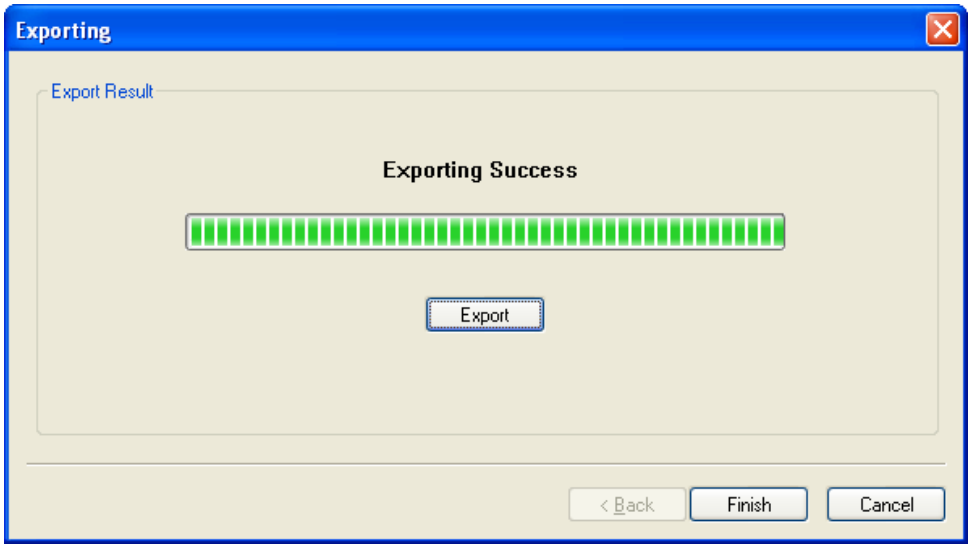
Log data can be exported to CSV file format using the **Export Report** button.

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.



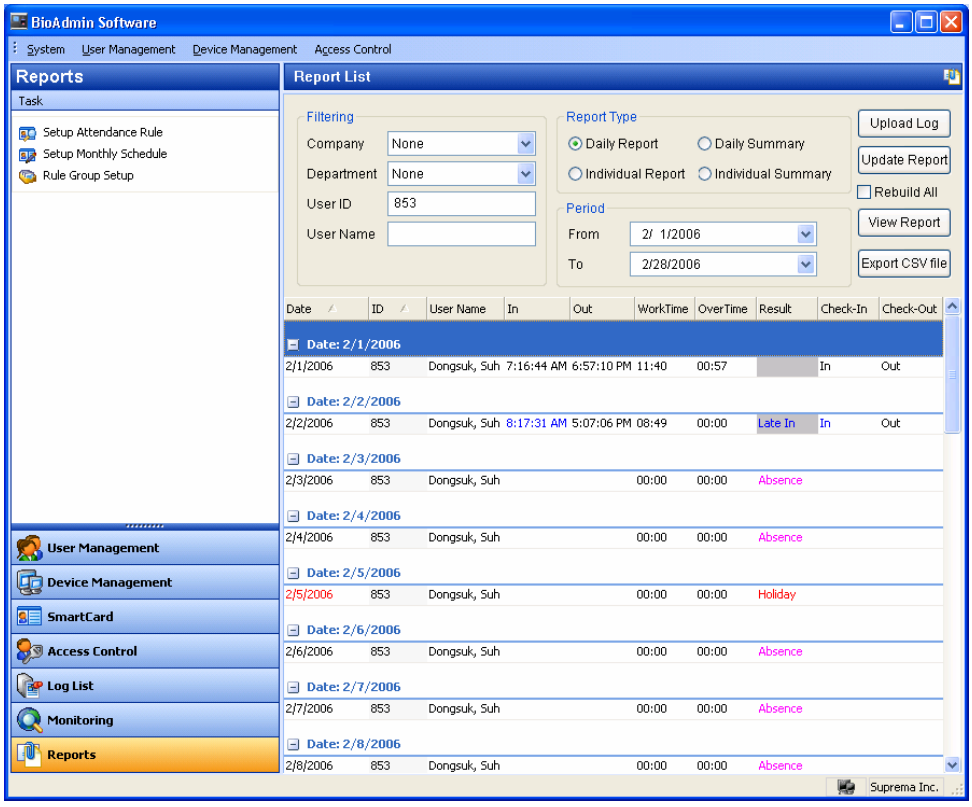
8.2.6. Delete Log information

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

9. Reports

Repot menu includes the followings operations.

- Set up attendance rule
- Upload log from device and create T&A event report.
- Export a created report to file
- Print created report



9.1. Configuration of reports page

Repot list page consists of 2 elements:

- Repot list page

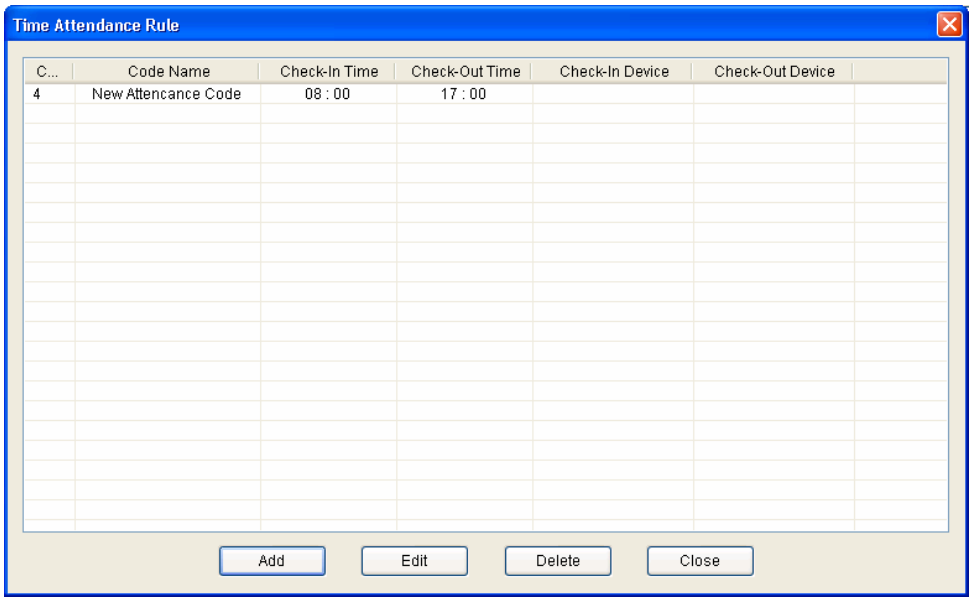
  Repot list shows menus setting filtering, report type, period and basic information required for creating a report.

- Task box

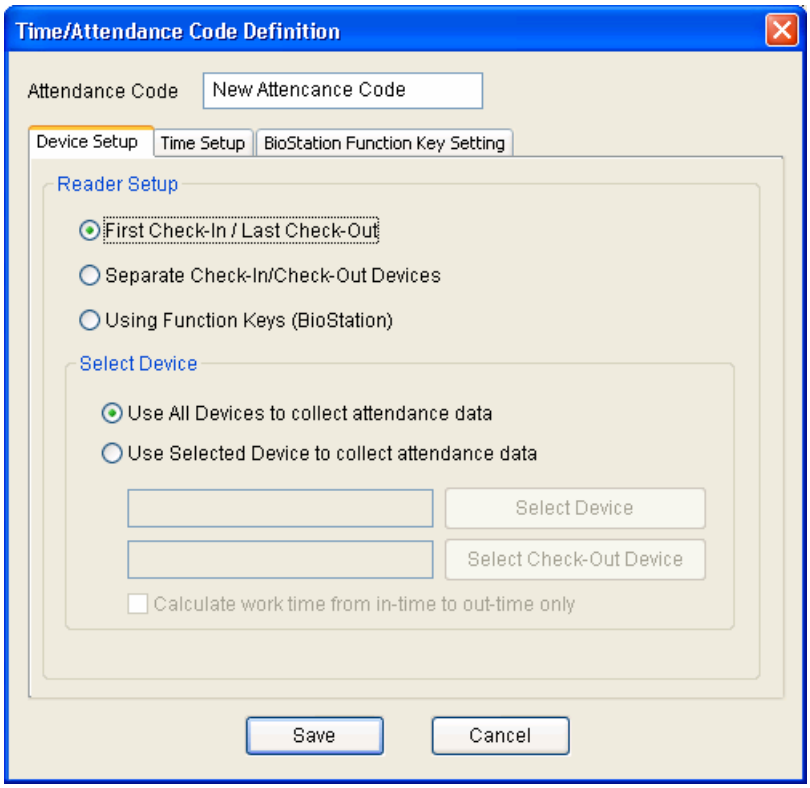
  Task box has buttons to set T&A rule.

9.2. Setup attendance rule

- Press **setup attendance rule** button to set a new T&A rule.



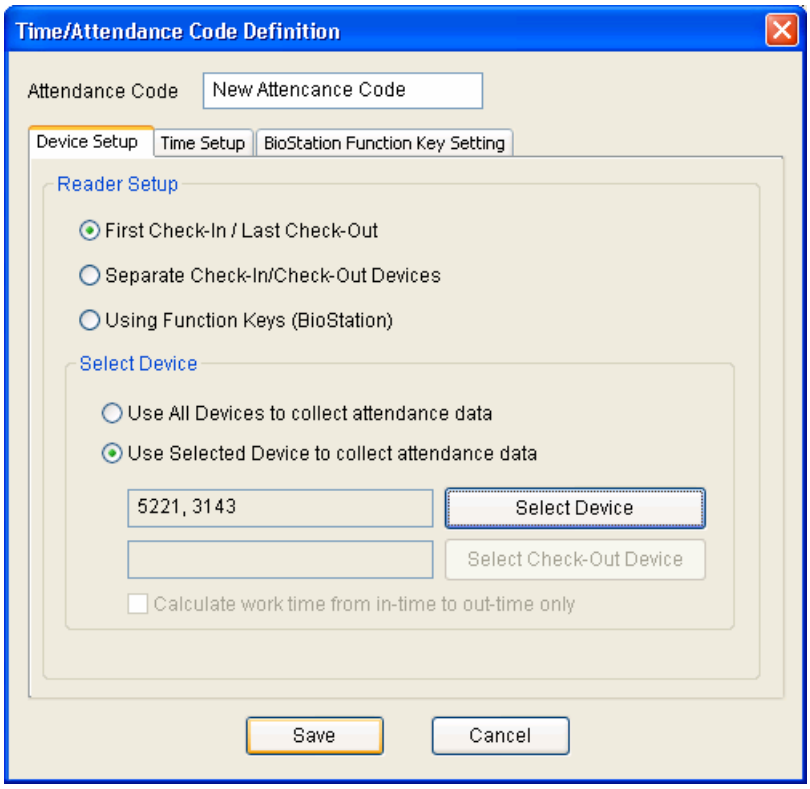
- In case of pressing add button, time attendance rule window appears.



- Enter attendance code.

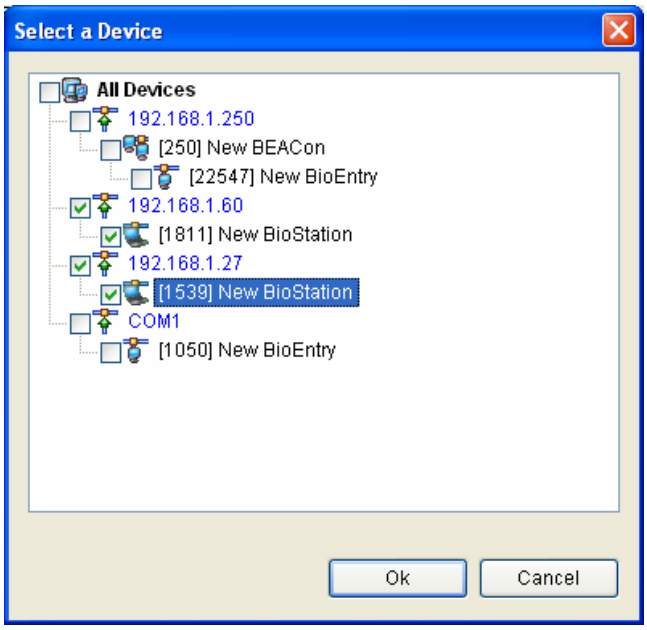
9.2.1. Device setup

Select device setup menu on time attendance rule page and set In/Out input device as below.



- In case of choosing **first check-in/last check-out**, user applies first authorized time as check-in and last authorized time as check-out.
- In case of choosing **separate check-in/check-out device**s, check-in/check-out devices can be designated separately using select device menu. In that case, limited to check in device, first time is applied as check-in and limited to check-out device, last time is applied as check-out. In case user inputs check-in or check-out for unselected device, log information is indicated as check-in or check-out but when creating a report, check-in or check-out is not applied.
- **Using function keys (BioStation)** – In case of choosing u**sing function keys (BioStation)**, limited to the cases when T&A key set in BioStation, it is applied to a report as check-in or check-out. This menu is applied only to BioStation. Therefore, BioEntry can't be used as T&A device in this case.

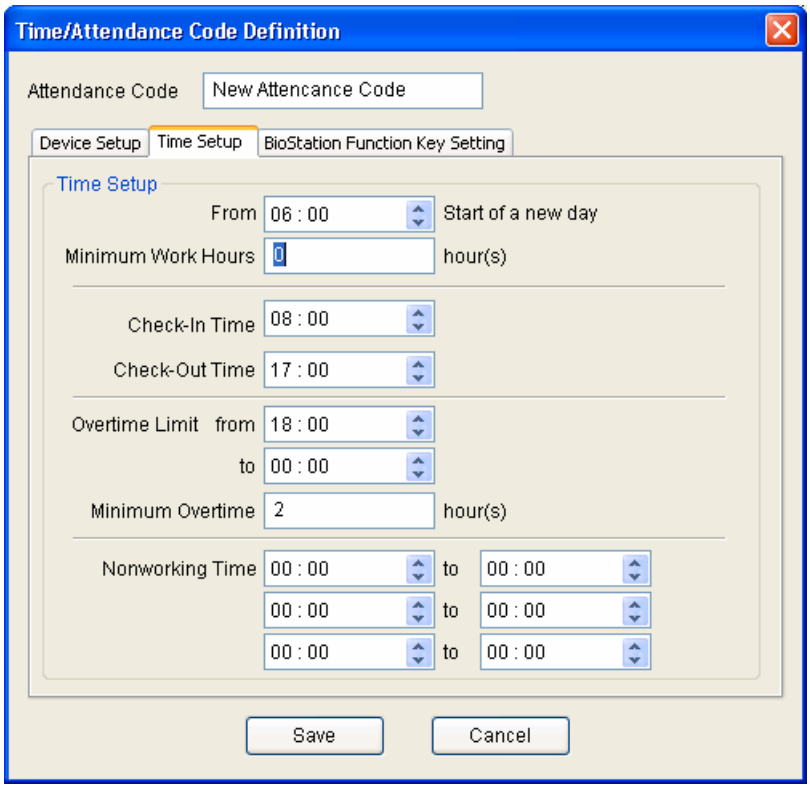
User can choose a device for T&A use thru select device menu.



- In case of choosing **use all devices to collect attendance data**, all devices connected to network are used for T&A device. However, in case of choosing **using function keys (BioStation),** BioEntry can't be used for T&A device.
- In case of choosing **use selected device to collect attendance data**, only selected device can be used for T&A device.

9.2.2. Time setup

Select time setup menu on time attendance code definition page and set time attendance time as follows.



Detailed setting process is as follows

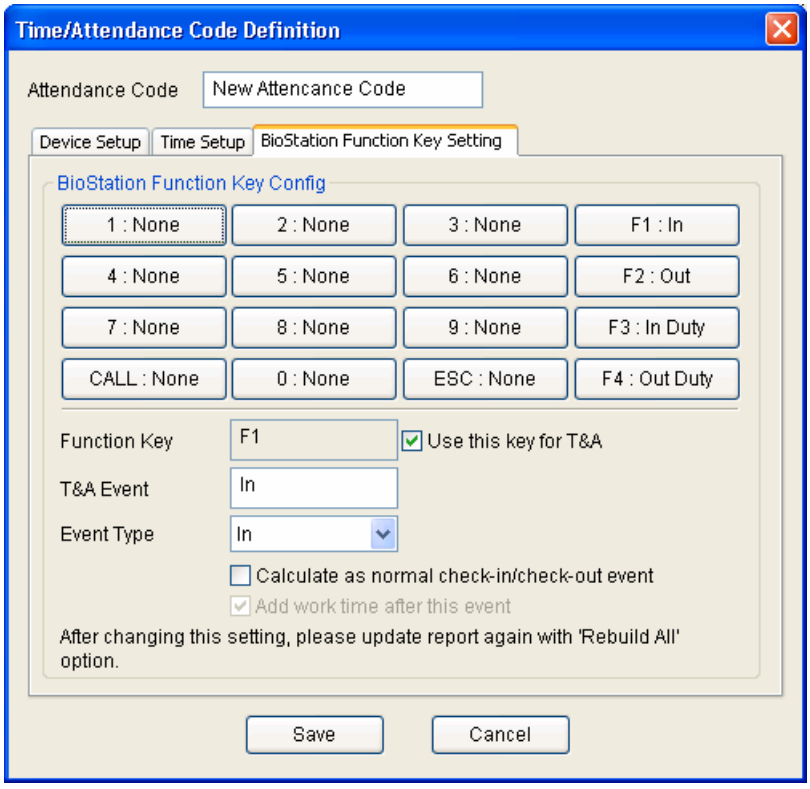
- Set standard time of work start in **from ----- start of a new day**
- Set minimum work hrs of applicable day in **minimum work hrs**. In case work hrs is less than set minimum work hrs, absence is applied to report. In case of setting minimum work hrs as 0, this function may not be used.
- Enter **check-in time**.
- Enter **check-out time**.
- Enter **maximum overtime hours**. In case one works overtime more than set maximum OT hrs, such hrs are not included in report as OT.
- Enter **minimum overtime hours**. In case of working overtime less than set minimum overtime hours, such hours are not applied as overtime in report.
- Set up **Nonworking Time** to exclude certain period of time from work time. This time will not be included in the working hour on report. You can select up to three Nonworking Time and see the Nonworking Time by using the drop down menu.

Note : Drop down menu on Nonworking Time is not to select a certain

Nonworking Time among the three Nonworking Times, but to just show the time setting of the Nonworking Time. Thus, once you set up two or three Nonworking Times on this menu, all of those Nonworking Times will be excluded from the working hour on report.

9.2.3. BioStation function key setting

On time attendance code definition page, select BioStation function key setting menu and set log information and report display as below.



Detailed setting process is as follows:

- Select applicable key.
- In case of using selected key as T&A key, check on **Use this key for T&A**.
- Input **T&A event** for selected function key. Upon Monitoring and log check,

input in T&A event for applicable key is displayed.

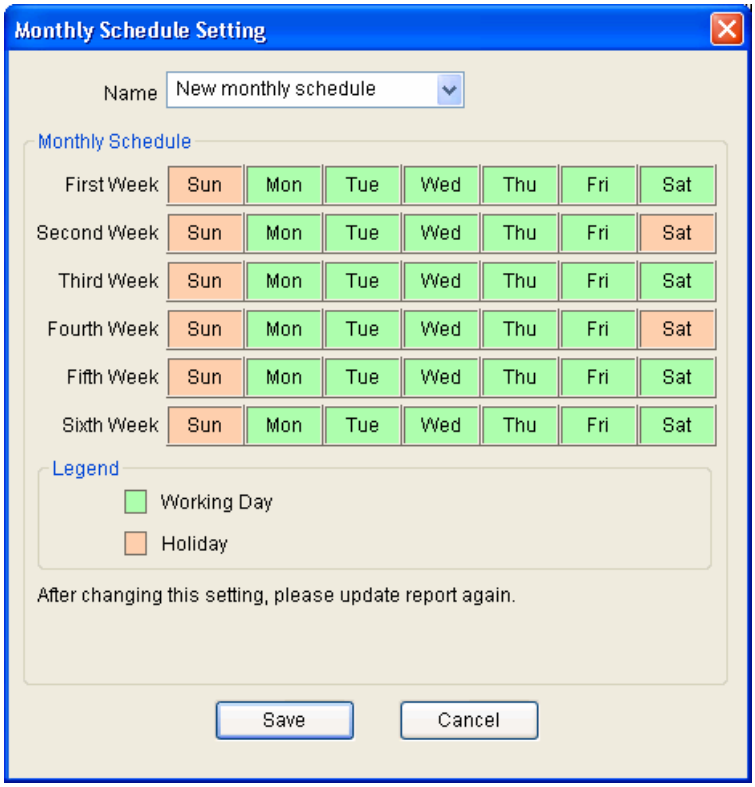
- Select Even Type among Check-In, Check-Out, In, Out. Selected events are used as basis of T&A result and computation of work hours.
- If you do not want to apply Late-In or Early-Out to a specific key, check on **Calculate as normal check-in/check-out event.**

> Changes will apply only when report is updated after changing BioStation function key setting.

9.3. Setup Monthly Schedule

By setting monthly schedule, you can select working day and holiday, which are used as a basis of T/A report. On holiday, late-in, early-out, absence are not applied. Work hours on holiday will be added to the holiday work time.

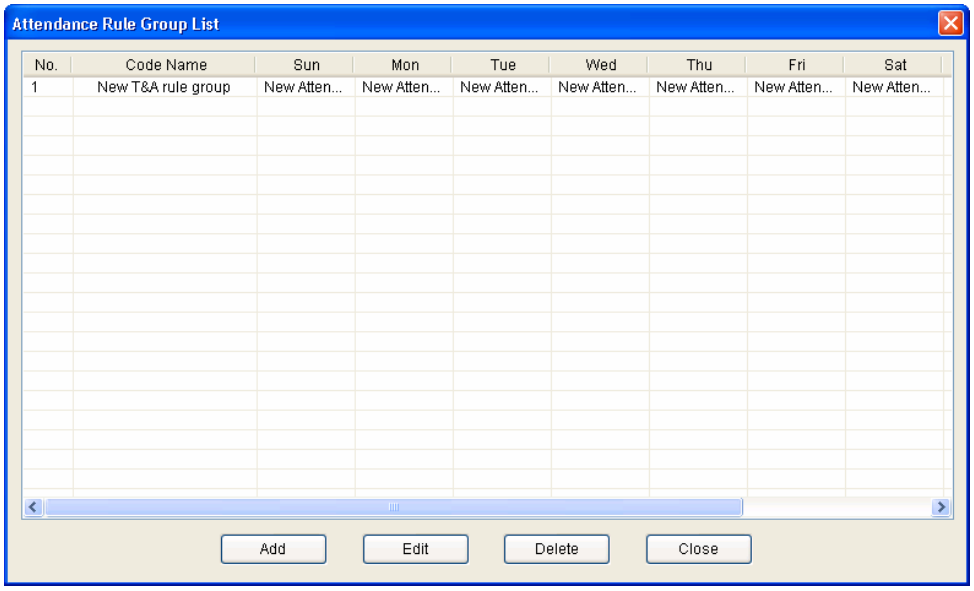
- Press **Setup Monthly Schedule** button.



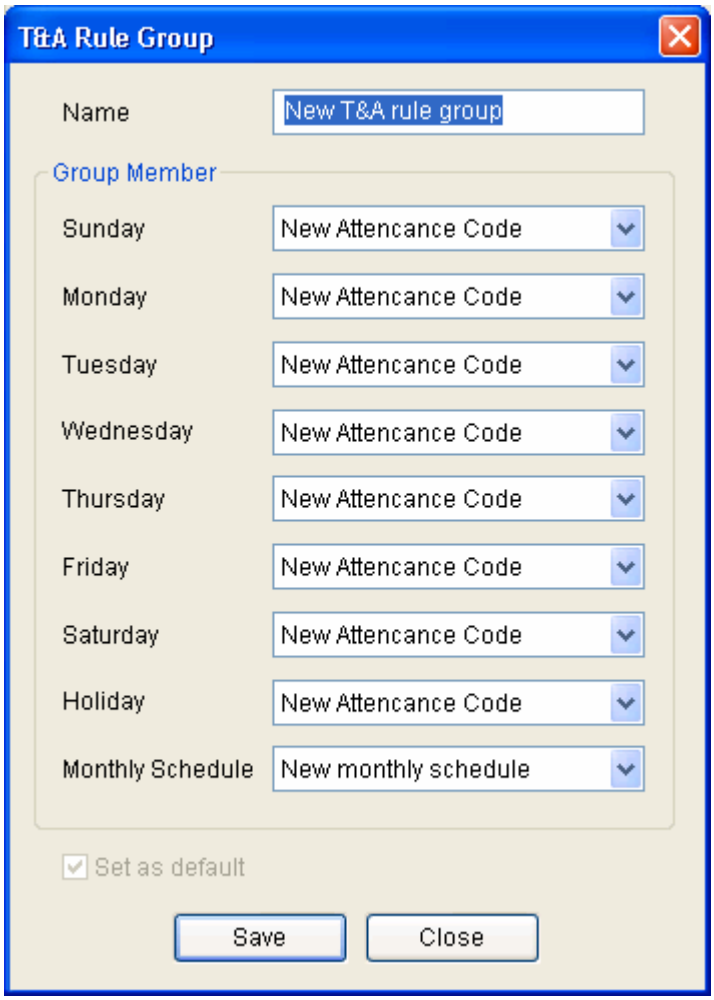
- Select Working Day and Holiday and press **Save** button.
- To apply new monthly schedule to T/A report, check on the **'Rebuild All'** of the Report List window and press Update Report button.

9.4. Group Configuration for T&A Control

You can make a group for the rules on T&A event control using the above configuration.



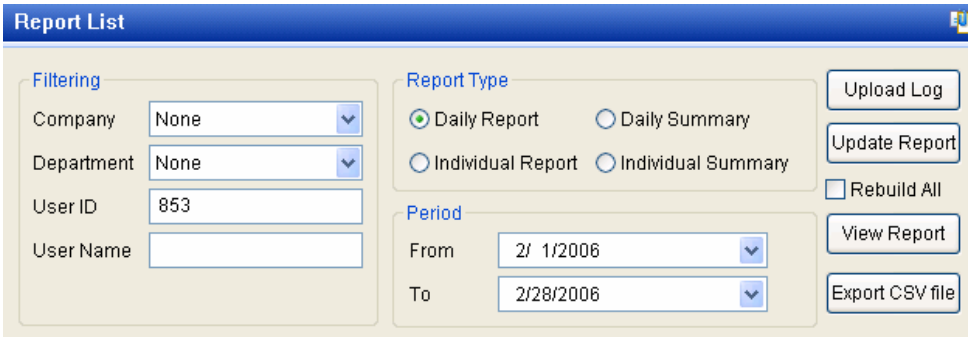
Press “Add” button to generate new rules on T&A group and configure each specific rule.



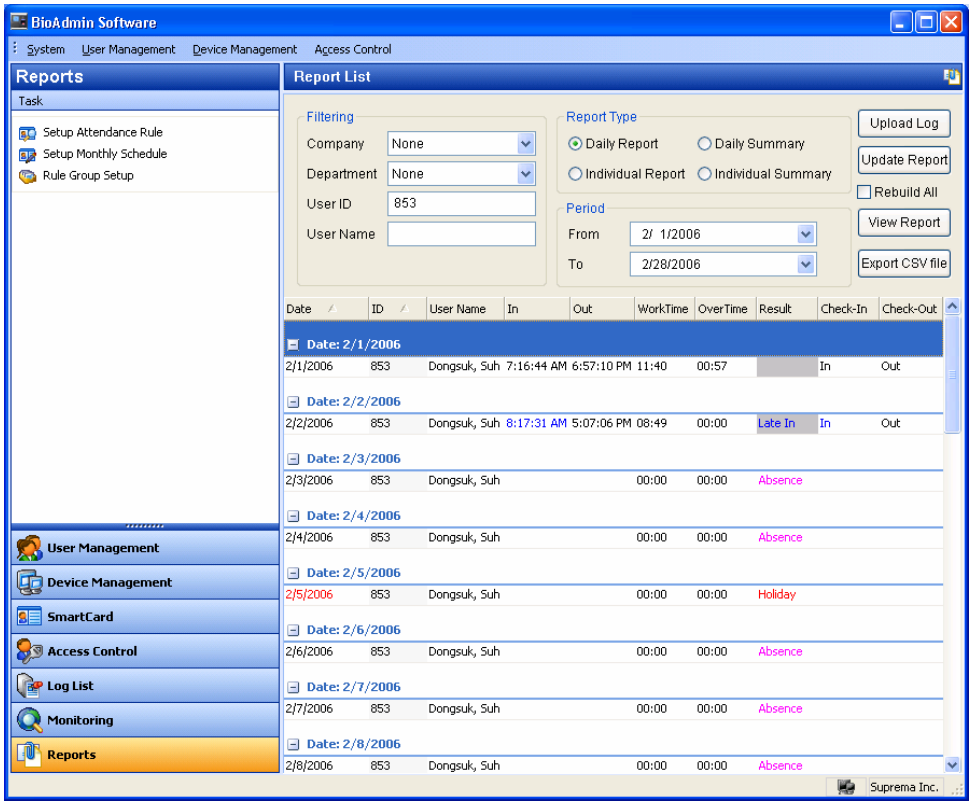
9.4.1. Use as default

By checking on **set as default**, apply selected T&A rule as basic rule. In case T&A rule is not set for certain users, basic rule applies to such users.

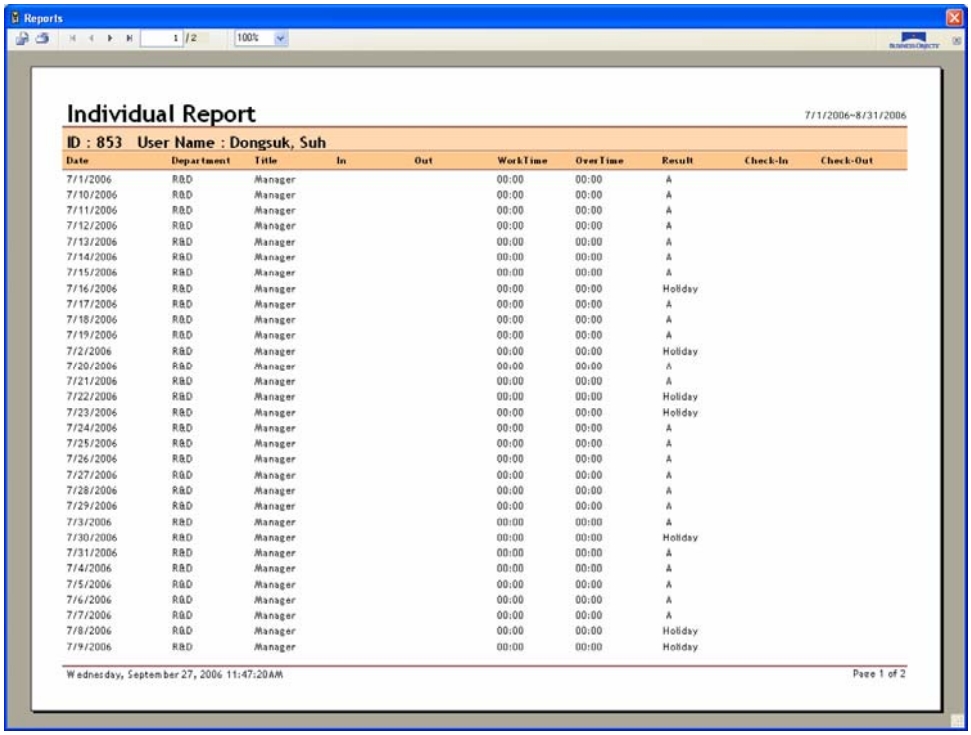
9.5. How to prepare report



- Press **upload log** and import the latest log information. This process is to create a report based on the latest event logs, so even after completing upload log, log is not displayed on report list.
- Select company, dept. and user on setting (filtering) menu to creating a report.
- Choose either daily report or individual report on type menu.
- Choose start date and finish date of report on period menu.
- Press **update report** button.



- Press **view report** button.



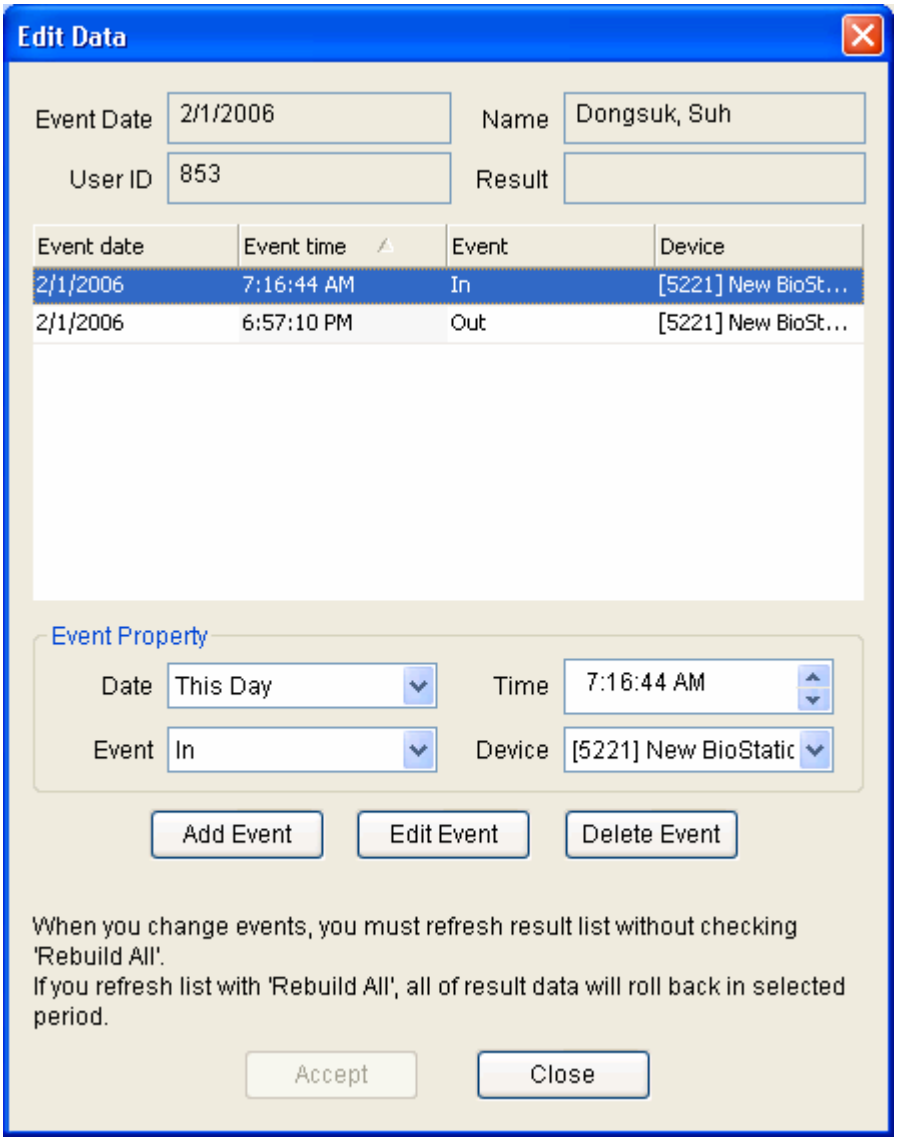
- Press  to save a file in varying formats.

- Press  to print out the report.

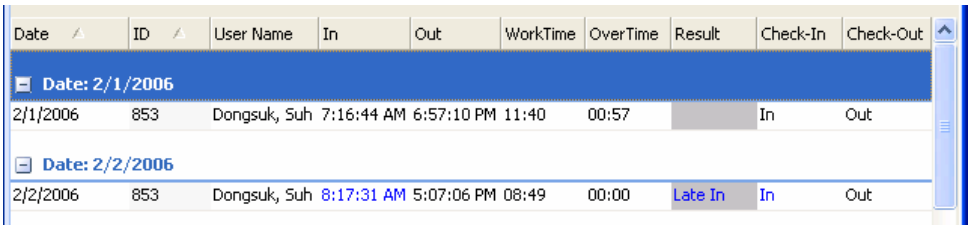
9.6. Edit Data

If necessary, administrator can add or correct user's T/A data.

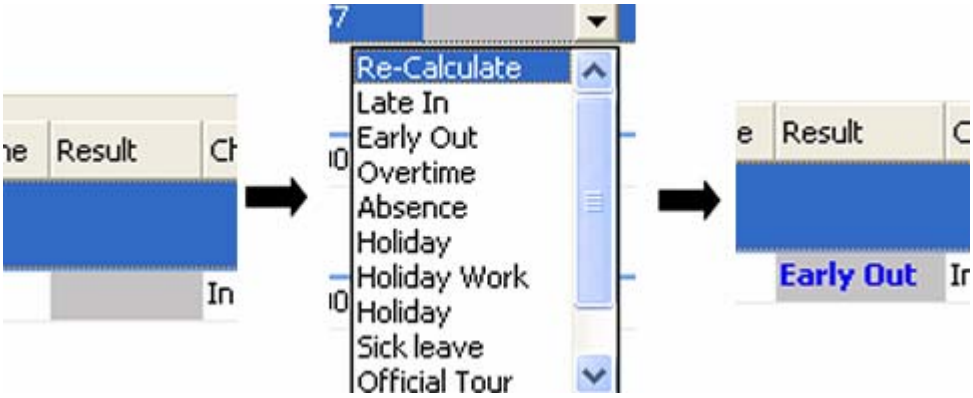
- If you double click a specific T/A data on daily report or individual report, Edit Data window will be initiated.



- Enter desired event values on the **Event Property** box and press **Add Event** or **Edit Event** button.
- Press **Accept** button to apply the corrected data to T/A report.
- The changed events are displayed as “Result” field in grey color.



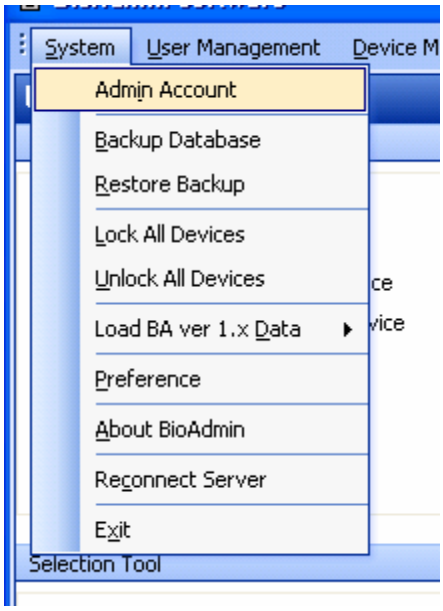
- The result can be modified at the report. By clicking “Result” of the report, the list to select displaying result will be shown as above figure, which is appeared on bold strokes and verified the changes easily.



Note : After correcting report data, you should press **Update Report** button without checking on ‘Rebuild All’. If you check on ‘Rebuild All’, T/A data will return to the original data before such correction.

10. Menu bar functions

10.1. System



10.1.1. Manage admin account

Add administrator to log in the BioAdmin or change password / user level of an existing administrator.

10.1.2. Data backup

Make manual backup file as well as auto backup file on the option menu. Backup file is saved as date-serial number format at the server installed a path.

10.1.3. Data recovery

After BioAdmin software modified to server/client type, data recovery is possible to copy backup file to server installed PC.

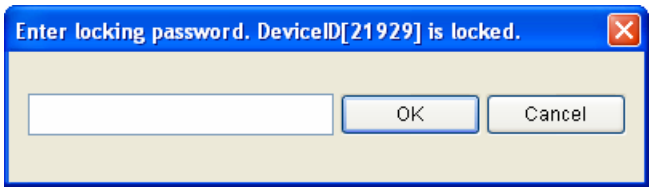
To recover a data, previously created backup file should be existed. By coping the file in the created folder as data-serial number type at the server installed path, all data can be restored as original backup status. All administrator & user information, rules, and log history are restored at the corresponding point, but data after restoration will be disappeared.

10.1.4. Lock all devices

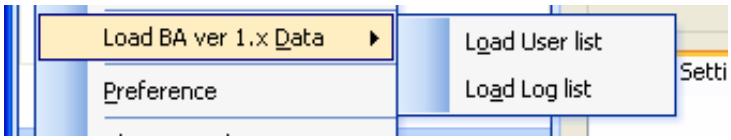
Lock/unlock linked all BioEntry and BioStation while using BioAdmin software. If administrator clicks lock all devices menu, all linked BioEntry and BioStation are locked and once locked, they don't react to any external packet except unlock command. In case of BioStation connected to the server, lock device does not support.

10.1.5. Unlock all devices

By clicking 'unlock all devices' menu, user can unlock all locked BioEntry and BioStation. If lock password has been set, user needs to enter password to unlock.



10.1.6. Load BioAdmin 1.X data



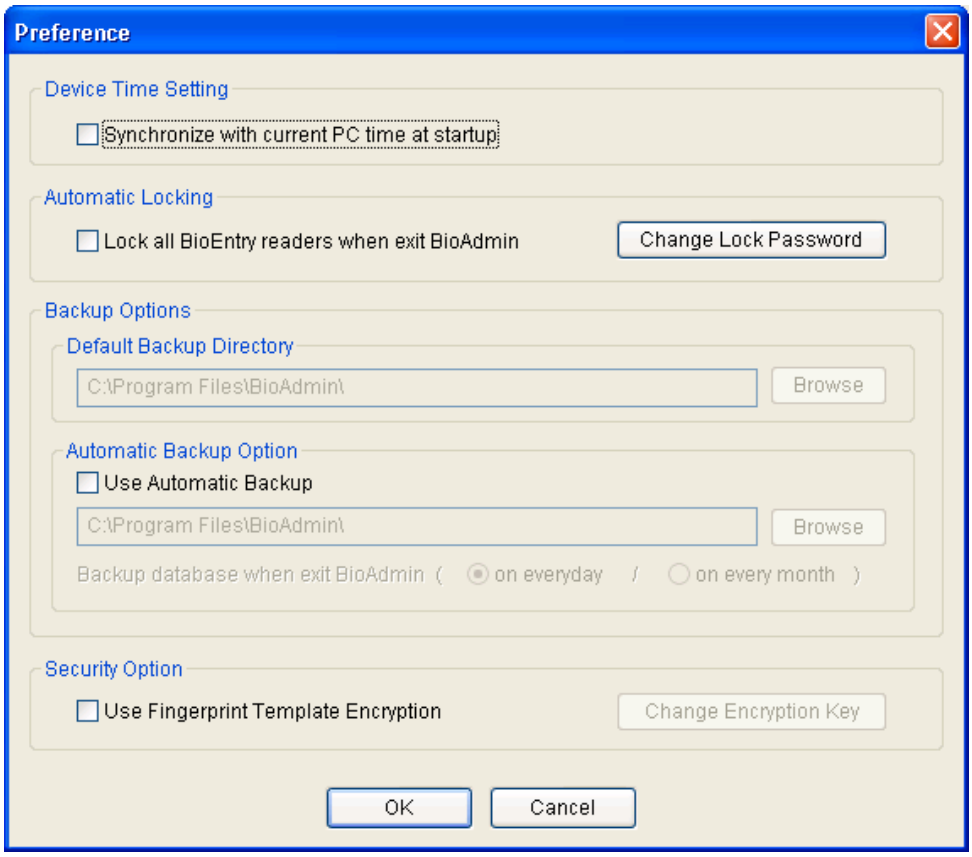
- Click **Load BioAdmin 1.X** data menu to import previous user data and log data generated while using BioAdmin software version 1.

> Note : This menu can be used at a time of first execution of BioAdmin software version 3.0 only. It is because data is created anew after deleting existing data when importing previous data running this menu.

10.1.7. Preferences

Preferences menu supports the following functions.

- Device Time Setting
- Automatic Locking
- Backup Options
- Security Option



- Device Time Setting

  By checking **synchronize with current PC time at startup** on preference window, administrator can set time of linked all devices by host PC time.

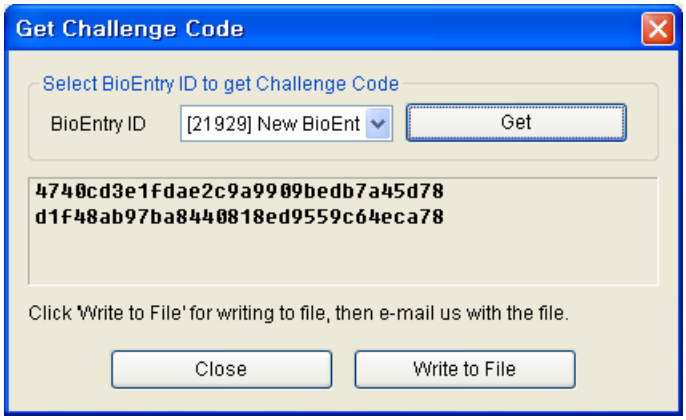
- Automatic Locking

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

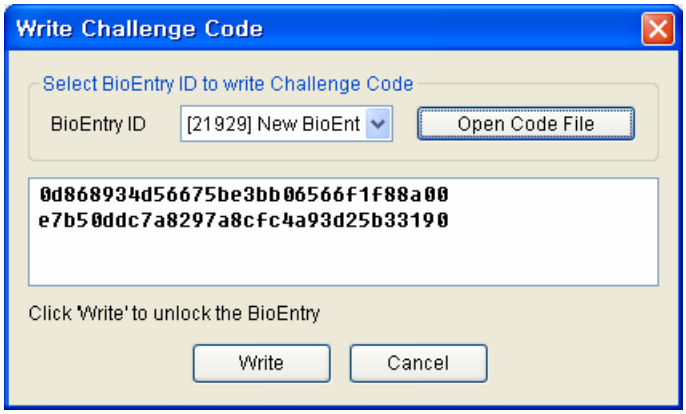
  - Lock password of BioEntry and BioStation can be changed by pressing change button and entering old and new password.

Note : As BioAdmin software doesn't save lock password, administrator should remember the password when using lock mechanism.

- Resolving the locked devices. If the devices 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)



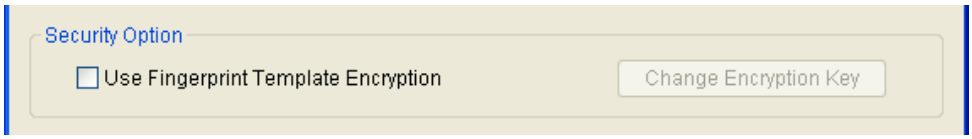
- The support team will send you the unlock code file corresponding to the challenge code. Use **Unlock a BioEntry and Password** to the **Default** button to resolve the device. Then, the device is unlocked and password is changed to default (null).



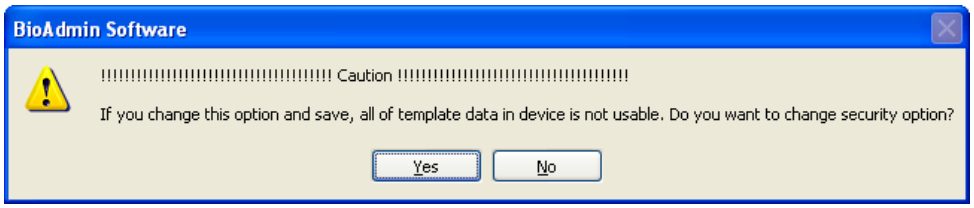
- Backup Options
  - Default backup directory: Default backup directory for database can be specified on the preference page. Related backup files will be stored on the specified directories. In case of BioAdmin Software v4.0 above, this option cannot create a backup path, but backup file at the server installed path.
  - 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. In case of BioAdmin Software v4.0 above, the backup file is created at the server installed path, which is similar to manual backup.
  -
  - 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.

Note : automatic backup option saves data on the basis of closing BioAdmin software. Thus, in case of not running BioAdmin or not closing BioAdmin after running, data is not saved.

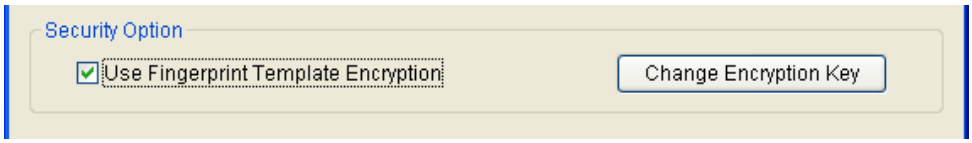
- Security Option
  - Security option is used to encrypting fingerprint template data which is used between host PC and BioStation. By encrypting the template data, you can enhance the security level of of the system.
  - Security option should be used only when there is no fingerprint data on the BioStation. Otherwise, BioAdmin will remove all fingerprint templates on the BioStation.



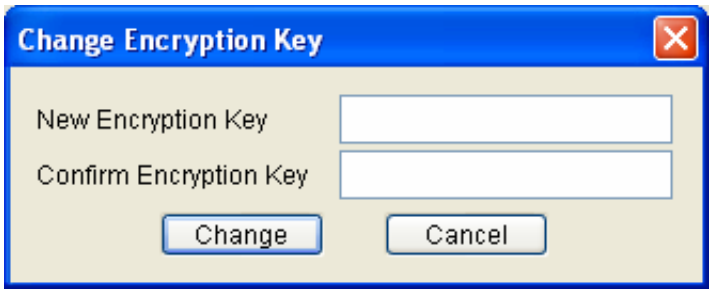
- Check on the **Use Fingerprint Template Encryption**.
- If you select the encryption option, a warning message will appear. If you want to continue the encryption, press **Yes** button.



- Press **Change Encryption Key** button.



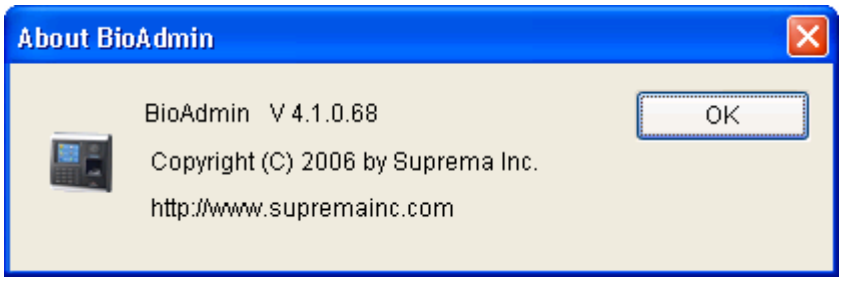
- Enter **Encryption Key**.



- Press **Change** button in **Change Encryption Key** window.
- Press **OK** button in **Preference** window.
- If you press **Cancel** button in **Preference** window or if the data encryption is interrupted by a network error, system will return to its earlier status before encryption.

- Whenever you change the encryption key, you need to apply the new encryption key for each of the connected BioStation. Also, you need to do so whenever you add a new BioStation to the network. Because encryption process will remove the existing user's templates on BioStation, you need to transfer the user's templates to the BioStation after finishing the encryption.
- When you use the encryption function, It is highly recommended to change the encryption key.
- Encryption key should be less than 31 digits.
- If the encryption is interrupted by a network error or by power failure, restart the BioAdmin program. Then, BioAdmin will automatically transfer the encryption setting to the remaining BioStation devices.
- You should be very careful in using the encryption function. If you are set different encryption key among BioStation devices, you may not be able to use the user's template compatibly among those devices.
- If the encryption key on host PC is different from that of BioStation, or if only either of host PC and BioStation is using the encryption option, following warning message will appear whenever such device is found on the network. If you press **No**, such BioStation devices will be disconnected from the network.

10.1.8. BioAdmin information



About BioAdmin on menu bar represents information on BioAdmin in use.

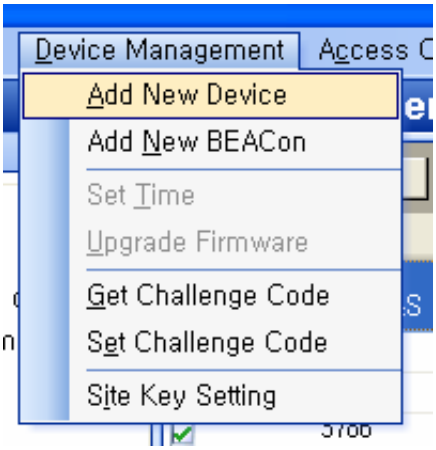
10.2. User Management

User management menu on menu bar supports following functions.

- Add New User
- Company Management
- Department Management
- Title Management
- Setup Custom Fields

For detailed setting, refer to ‘chapter 5, user management’

10.3. Device Management

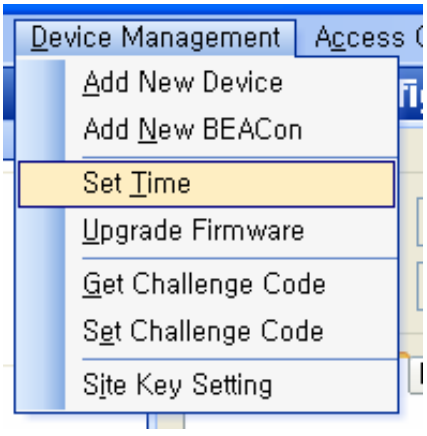


Device management menu on menu bar supports following functions.

- Add New Devices
- Add New BEACon
- Set Time
- Upgrade Firmware
- Get Challenge Code
- Set Challenge Code
- Site Key Setting

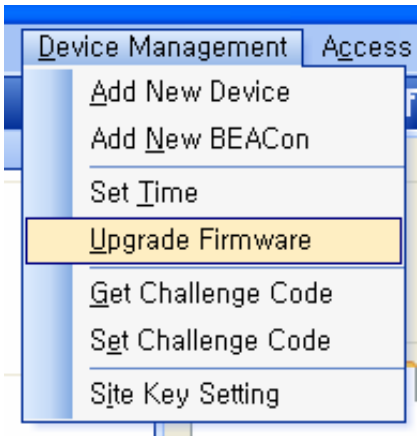
For detailed setting as to add new device, add new controller, import factory password code, factory password (password initialization), refer to 'chapter 6, device management'.

10.3.1. Time setting

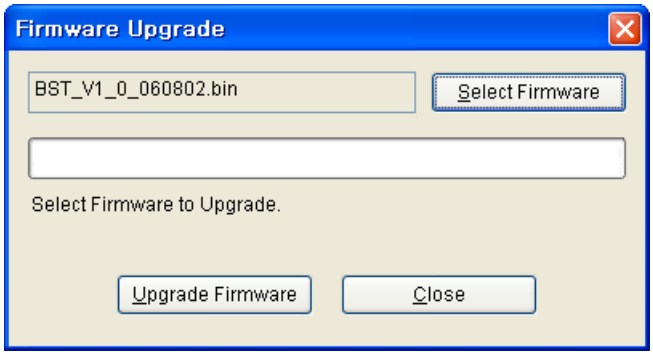


- You can synchronize the time of all of the networked BioEntry™ to the time of host PC. If you already checked on the S**ynchronize current PC time at startup check box**, which is on Options → Preference → Device Time Setting, you do not need to synchronize the time on this menu.

10.3.2. FW upgrade



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

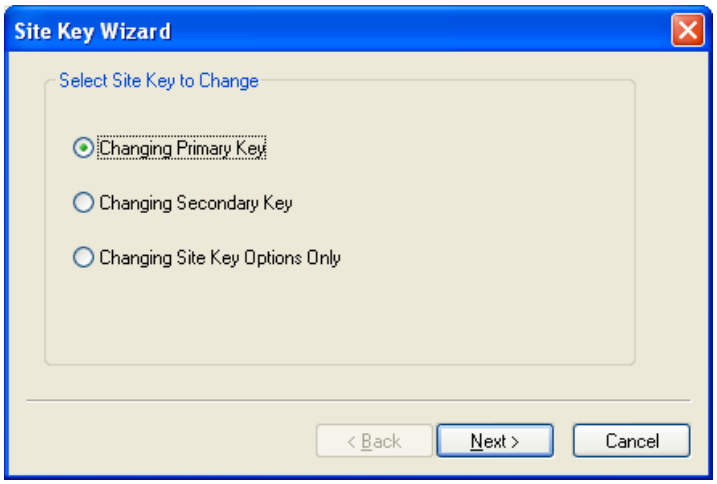


- Select a firmware file by clicking the **Search Firmware** button.
- Execute upgrade by clicking the **Upgrade Firmware** button.
- If BioEntry or BioStation is turned off or reset in the process of upgrading, restoration might be impossible.
- Firmware upgrade is processed for one device. Selection of a group or all devices is not allowed.

For detailed setting, refer to chapter 5 'user management'.

Note : Once firmware upgrade is complete, BioEntry and BioStation are rebooted automatically and connected to network. It is recommended not to do any other operation for about 5-10 sec after BioEntry or BioStation are rebooted due to upgrade.

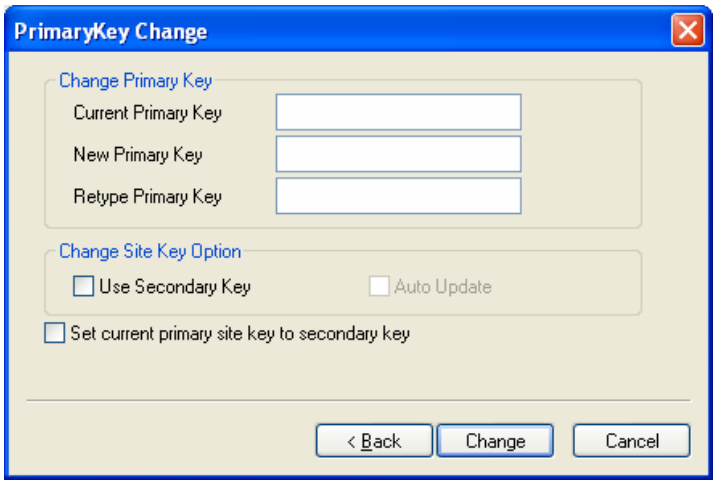
10.3.3. Site Key Setting



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

Note : ***Site keys should be handled with utmost caution. If it is revealed, the whole system is not secure any more.***

- Primary Key

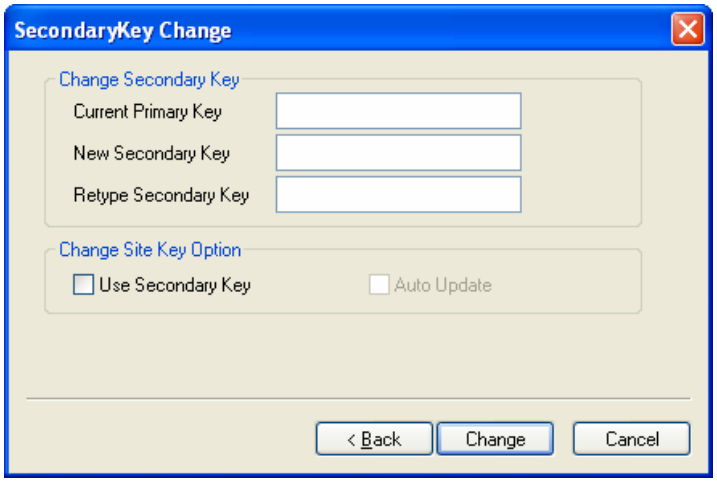


To change the primary key, you should enter the current and new primary keys. Besides the **Auto Update** option, you can also select the following options.

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

- Secondary Key

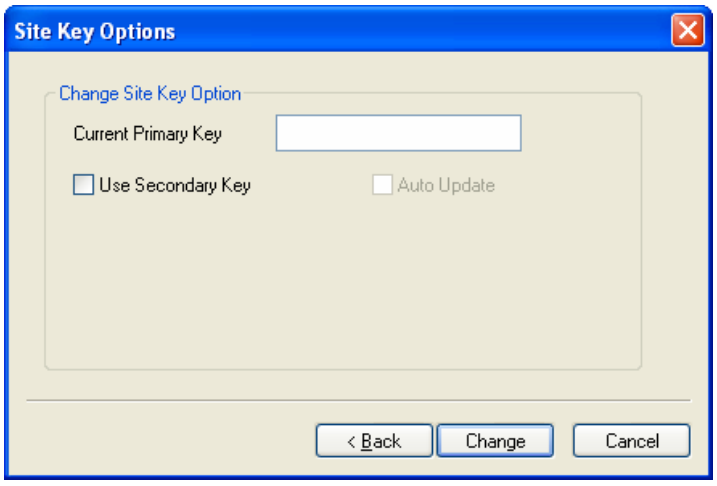
  To change the secondary key, you should enter the current primary key and the new secondary key.



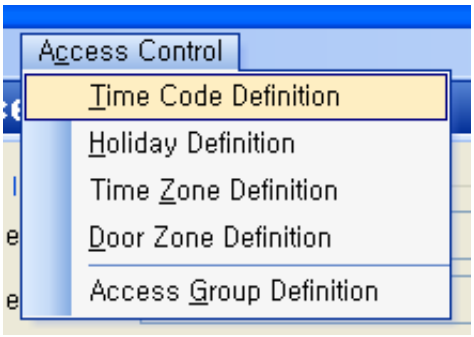
- Key Options

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

the current primary key with the options.



10.4. Access (I/O) Control



Access control menu on menu bar supports following functions.

- Time Code Definition
- Holiday Setting
- Time Zone Setting
- Door Zone Setting
- Access Group Setting

For detailed setting, refer to chapter 8, access control.

Contact Information

Suprema Inc.
16F Parkview Office Tower, Jeongja-dong, Bundang, Seongnam, Gyeonggi, Korea
Tel : +82-31-783-4502
Fax : +82-31-783-4503
Website : http://www.supremainc.com
Sales inquiry : sales@supremainc.com
Technical inquiry : support@supremainc.com

