BioStar 1.93
Administrator Guide

EN 102.00.BS V1.93A

suprema

BioStar 1.93 Administrator Guide

Warranty and Disclaimers

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 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 that is returned to Suprema within the Warranty Period, with 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 that 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 (Return Material Authorization) 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 Product. The report should include full details of each defective product, model number, invoice number, and serial number. No product without an RMA 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 and 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, lifesaving, or 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, 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." Supreme 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 before placing your order.

Copyright Notice

01 About the BioStar System

BioStar is Suprema's next-generation access control system, based on IP connectivity and biometric security. Most system devices integrate fingerprint scanners and card readers for multiple levels of user authentication. However, Suprema's biometric devices, installed at each door, work not only as card or fingerprint scanners and card readers, but also as intelligent access controllers.

The licensed standard edition of BioStar is unlocked by a USB dongle. Without the dongle, BioStar functions as a free, but limited-capability version. With the dongle, BioStar offers greater versatility and additional features, as shown in the table below:

	Standard Edition	Free Version
Maximum # of doors	512	20
Maximum # of clients	32	2
Zone support	Yes	No
Email notifications	Yes	No
Server matching	Yes	No
Shift types	Daily and Weekly	Weekly only
IO board	Yes	No
Visual Map	Yes	No

1. About the BioStar System

BioStar V1.93 supports the following devices:

- **BioStation A2**: This fingerprint recognition device is developed based on SUPREMA's newest fingerprint recognition technology and hardware platform. This device supports all functions regarding access control and attendance management, including authentication speed of up to 150,000 people per second, Live Finger Detection (LFD) function, face detection, PoE and attendance management.

- **BioStation 2**: This device enables high-speed matching and powerful authentication performance using SUPREMA's upgraded biometric recognition technology and high performance CPU as well as high-speed transmission of massive data. This product features luxurious external design and an IP65-rated waterproof and dustproof structure so that it can be installed in various environments.

- **BioStation L2**: BioStation L2 is a fingerprint recognition device that provides both access control and attendance management functions. Up to 100,000 templates can be saved and this device provides a process speed of up to 100,000 people per second, Live Finger Detection (LFD) function, and attendance management function.

- **BioEntry W2**: BioEntry W2 is an access control and time & attendance device in which Suprema's latest hardware and software coexists. This device mounts a quad-core CPU, 2GB of memory, OP5 sensor, and the latest fingerprint algorithm. It can match 150,000 fingerprints in a single second. It also includes live fingerprint detection (LFD) and time & attendance features to provide excellent performance. This device can be used in various environments since the device has a small width size of 50mm and IK08 rated vandal-proof, and IP67 dust & water proof structure. This device also provides added flexibility in system design feature multi-card support with dual-frequency RFID technology.

- **Secure I/O 2**: This is a separable controller with an ultra slim design for one external door relay control and input and output expansion. It is used with SUPREMA's IP access control terminals and encrypted communication, reinforcing security and providing an optimized solution according to the service environment.

1. About the BioStar System

- **BioStation (V1.5 or later)**: BioStation is a multifunctional terminal with a keypad and a 2.5-inch color LCD monitor that allows you to perform user enrollment and administration functions directly from the device. BioStation can be connected to a network via a wireless LAN or Ethernet and includes USB host and device interfaces for easy data transfer. BioStation MIFARE (BSM) models also support entry control via smart cards.

- **BioStation T2**: BioStation T2 is a multifunctional, IP-based access control terminal with a camera, 5-inch touchscreen, fingerprint scanner, card reader, and built-in video phone feature.

- **FaceStation**: FaceStation is a multifunctional, IP-based access control terminal with an LCD touchscreen and a camera for face recognition and videophone functions. FaceStation supports multiple interfaces for connecting to computers or networks and access controls via Wiegand and I/O ports. In addition, the device allows for authorization via multiple access cards.

- **BioEntry Plus (V1.2 or later)**: BioEntry Plus is an IP-based access control device that includes both fingerprint recognition and entry via access card. The device can be controlled independently via command cards or managed entirely via the BioStar interface. BioEntry Plus can be connected to electric door strikes via an internal relay or used with the Secure I/O device for extra security and expanded capability.

- **BioEntry W** : The BioEntry W includes all of the features of the BioEntry Plus in a vandal-resistant, IP65-rated structure. BioEntry W is ideal for outdoor installation, with exceptional durability in harsh environments. It features extensive communication interfaces and PoE capability.

- **BioLite Net (V1.0 or later)**: BioLite Net is IP-based fingerprint terminal designed specifically for outdoor use. With a rugged, IP65-rated waterproof structure, it offers extra durability to withstand the elements. As either a simple door control or part of a complex, networked environment, BioLite Net supports the full functionality of BioStar's time and attendance and access control features.

1. About the BioStar System

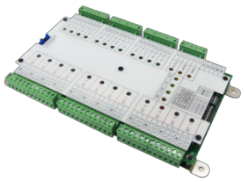
- **Xpass**: Xpass is an IP-based access reader/controller designed exclusively for use with RF cards. It provides many similar functions to the BioEntry Plus device, but is waterproof for outdoor use and can be connected and powered by a single CAT5/6 cable.

- **Xpass S2**: The Xpass S2 device is a slimmer version of the Xpass that supports FeliCa and ISO 15693 cards. Its low profile allows it to be installed in tight spaces and it features access control to floors when connected with a LIFT I/O device via RS485 slave.

- **X-Station**: X-Station is an easy-to-use smart IP terminal with a 3.5-inch touchscreen LCD that supports ID and card access only. The device supports face detection with a built-in camera. X-Station allows you to store up to 200,000 users with 1GB of internal flash memory and 256MB of RAM.

- **BioMini/BioMini Plus/BioMini Plus 2**: BioMini series are fingerprint scanners that can be used for convenient user enrollment. Installing the device is simple: plug them into a USB connection on any computer that is connected to the BioStar server and install a driver.

- **Secure I/O**: The Secure I/O device provides a convenient way to increase the security of externally mounted devices or expand the capabilities of your system. When doors are controlled by a secure I/O device, intruders cannot open doors even if they succeed in uninstalling external devices. To further increase security, the secure I/O device provides encrypted communications between door components. The Secure I/O device has four input switches and two output relays to allow control of multiple components with a single device.



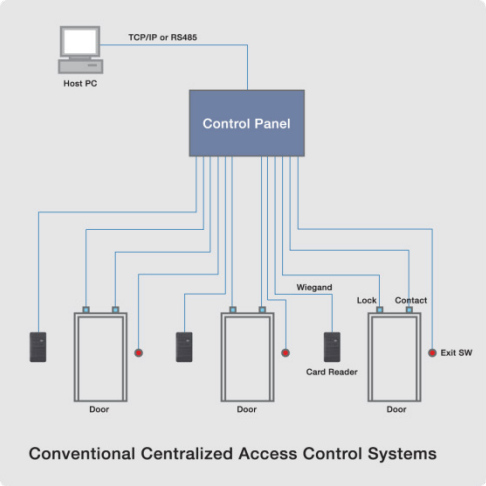
- **LIFT I/O**: The LIFT I/O supports 0-9 device IDs and 12 output ports (12 input ports are not currently supported). Each output can be connected to an elevator button to control access to floors. The LIFT I/O can be connected via RS485 as a slave to Xpass and Xpass S2 devices. Up to 10 LIFT I/O devices can be connected to a BioEntry Plus, Xpass or Xpass S2 device to control up to 120 floors.

1. About the BioStar System

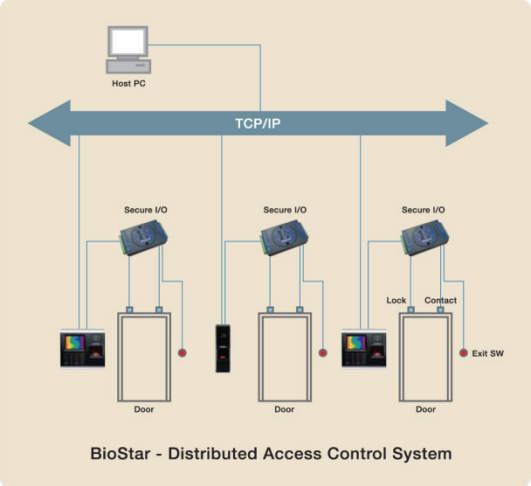
1.1 Logical Configuration

BioStar is a distributed intelligence system. Instead of the complex wiring and centralized control required by conventional access control systems, Suprema's access control devices can be connected via TCP/IP or wirelessly to a local area network or connected directly via serial connections. User information, access rules, and other data can be distributed to each device to speed up authorization time and provide continual operation even when the connection to the network is lost.

As the following graphic illustrates, the BioStar system does not require separate access controllers. This feature provides a distinct advantage over other access control systems, because BioStation, BioEntry Plus, or BioEntry W devices act simultaneously as both a controller and a reader. As a result, Suprema's distributed intelligence approach requires less hardware and less wiring than conventional, centralized access control systems.



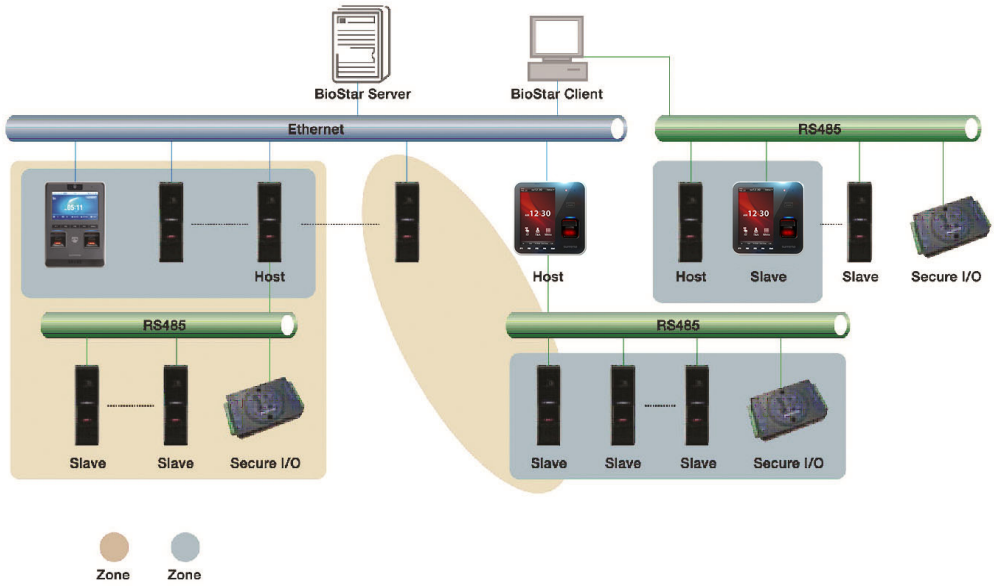
Conventional Centralized Access Control Systems



BioStar - Distributed Access Control System

BioStar is a server-client application that supports up to 32 clients (2 clients maximum in the free version). A typical configuration consists of numerous access control devices connected to a central server via Ethernet, WLAN, and/or RS485. BioStar is compatible with MS SQL Server and MySQL databases.

Overall, the system supports a maximum of 512 doors and 512 devices (20 doors and devices in the free version). Networked devices can be easily grouped together to create various combinations of anti-passback or alarm zones, as illustrated by the graphic that follows.



1.2 Access Control Features

The BioStar system goes a step beyond conventional access control systems, by combining unique biometric identification with configurable access card capabilities.

1.2.1 User Authentication

Suprema's access control devices incorporate advanced, award-winning fingerprint recognition algorithms to provide secure access control. The system allows for a wide variety of user authentication modes:

- **Fingerprint or access card**: either a fingerprint scan or access card may be used to gain entry.
- **Fingerprint + access card:** both fingerprint scan and access card are required for access.
- **User ID + fingerprint:** a user ID and fingerprint scan are used in combination; the user ID identifies the user and the fingerprint scan is used for authorization.
- **User ID + password:** a user ID and password are used in combination; the user ID identifies the user and the password is used for authorization.
- **User ID + card + fingerprint:** a user ID, access card, and fingerprint scan are used in combination.
- **Fingerprint only**: authentication via a fingerprint scan is the only method to gain entry.

- **Card only**: authentication via an access card is the only method to gain entry.

[FaceStation Only]

- **Face**: authentication via face recognition is the only method to gain entry.
- **Face + Password**: authentication via face recognition plus password.
- **Face + Card**: authentication via face recognition plus access card.
- **Face + Card or Password**: authentication via face recognition plus access card or password.
- **Face + Card + Password**: authentication via face recognition plus card plus password.
- **User ID + Face**: authentication via user ID plus face recognition.
- **User ID + Face or** Password: authentication via user ID plus face regognition or password.
- **User ID + Face +** Password: authentication via user ID plus face recognition plus password.

[BioStation A2, X-Station, BioStation T2, and FaceStation]

- **Detect face**: upon successful authentication, a face image is captured.

BioStar stores two templates of each fingerprint and up to two fingerprints per user (four templates total). If desired, one fingerprint can be used as a duress signal, to activate alarms or send alerts in situations where a user is required to gain access under duress. Duplicate templates of each print enhance authentication performance by reducing the likelihood of false rejections. For more information about registering fingerprints, see section 3.6.2.

BioStar also provides administrators with the ability to read EM4100 and HID proximity cards and read, issue, and format MIFARE® and iCLASS® access cards. For more information about access cards, see section 3.6.4.

BioStation A2, X-Station, BioStation T2 and FaceStation devices are equipped with cameras to allow for face detection and recording of face images for enhanced security. For more information about face detection, see section 3.6.3.

1.2.2 User Management

BioStar supports both manual and automatic modes for user management. Manual synchronization is available for enrolling different subsets of users to particular devices or when the total number of users in the BioStar database exceeds the limits of a device. Automatic synchronization is available when managing user records at the device is not required or desired.

BioStar collects log records from devices and allows the data to be exported to a delimited text file (.CSV) for custom reporting. The software supports an unlimited number of user records—the maximum amount of data stored is subject only to the capabilities of the underlying database and hardware configuration. For more information about user management, see sections 4.1, 4.2, 4.3, 4.5, and 4.6.

1.2.3 Access Group Management

BioStar allows administrators to build custom access groups by combining permissions for timezones and doors. With this capability, BioStar provides customizable, scheduled access control.

BioStar supports up to 128 timezones that consist of a seven day schedule, plus two holiday schedules. Each day in a timezone can include as many as five distinct time periods.

In total, BioStar supports up to 128 access groups that can be transferred to all connected devices. For more information about access groups, see section 3.8.

1.2.4 Device Management

Administrators can control multiple aspects of devices via the BioStar software. In addition to authentication behaviors, BioStar supports the configuration of inputs, output relays, actions, and sounds. The system includes options for customizing sound and display settings for BioStation A2, BioStation 2, BioStation L2, BioStation, X-Station, BioStation T2 and FaceStation devices, and LED & Buzzer settings for other devices.

The system provides configuration options for controlling external devices, such as door strikes and alarm sirens. BioStar can also connect to and communicate with third-party devices via a Wiegand interface. For more information about device management, see sections 3.2 and 4.7.

1.2.5 Door and Elevator (Lift) Management

BioStar allows for comprehensive control of doors and connected devices, such as door relays, alarm relays, door sensors, and exit switches. Each door can be operated by up to two devices and, when two devices are connected to a door, administrators can apply anti-passback controls. BioStar also allows for control of elevators (lifts) via BioEntry Plus, Xpass and Xpass S2 devices, with Secure I/O devices connected as slaves.

BioStar allows specific configuration of alarm events for doors that are forced open or held open longer than a specified interval, including activating alarm sounds from individual devices, sending signals to external alarm sirens, displaying warnings in the BioStar user interface, and sending e-mail notifications (not available in the free version). In addition, administrators or operators can remotely lock and unlock doors or reset alarms. For more information about door management, see sections 3.3, 4.3, and 4.4. For more information about elevator management, see section 3.4.

1.2.6 Zone Management

The BioStar system gives administrators complete control of various zones (not available in the free version). Zones can be created with devices connected via Ethernet or RS485 and can include a master device and up to 65 member devices. In addition, individual devices can be included in up to four zones.

BioStar supports zones for increased access control, such as anti-passback and entrance limit zones, as well as zones that provide control for alarm or fire alarm outputs and actions. BioStar also allows administrators to synchronize time, event logs, and user data for all devices in a specified zone. For more information about zone management, see section 3.5.

1.2.7 Time and Attendance

BioStar versions 1.2 and higher include time and attendance features to allow administrators to define time categories, shifts, daily schedules, and holiday settings. The T&A capabilities of BioStar can be used to enforce compliance with check-in and check-out procedures, restrict access to off-duty personnel, and report attendance data.

BioStar allows administrators to customize T&A functions for BioStation A2, BioStation 2, BioStation L2, BioEntry W2, BioStation, X-Station, BioStation T2 and FaceStation devices and to specify how events are recorded. The BioStar interface also allows administrators to monitor a user's check-in and check-out status in real time. For more information about time and attendance, see sections 3.9 and 4.6.

1.2.8 IP Camera and NVR Server Management

BioStar versions 1.5 and higher support internet protocol (IP) cameras and network video recorder (NVR) servers, to allow administrators to monitor areas and be notified of specific events with real-time still images transferred from the IP cameras. By interoperating with the NVR servers, the BioStar system can also display time-sorted event logs, together with recorded videos stored on the servers. From the BioStar interface, administrators can add and customize IP cameras and their functions. For more information about the IP cameras and NVR servers, see sections 3.11 and 4.1.

1.3 Functional differences between a 1.x device and a 2.x device

The firmware structure of SUPREMA's devices is different between devices which support BioStar 1 and devices which support BioStar 2. Therefore, a device which supports BioStar 2 cannot be connected and used with BioStar 1. However, BioStation 2, BioStation A2, BioStation L2 and BioEntry W2 among the devices only supporting BioStar 2 were added to be used in BioStar 1.

The following are the limitations that occur when connecting and using BioStation 2, BioStation A2, BioStation L2 or BioEntry W2 with BioStar 1. Check the following limitations before configuring the system.

Compatible 2.x Device

- BioStar 1.91: BioStation 2, BioStation A2, BioStation L2
- BioStar 1.92: BioStation 2, BioStation A2, BioStation L2, BioEntry W2
- BioStar 1.93: BioStation 2, BioStation A2, BioStation L2, BioEntry W2

Compatible Firmware

- BioStation 2: 1.2.1 version or later
- BioStation A2: 1.1.0 version or later
- BioStation L2: 1.0.1 version or later
- BioEntry W2: 1.0.0 version or later

User

- Import user: Department information and PIN cannot be imported.
- Card: A security credential card, which could be issued in BioStar 2, cannot be issued. In addition, only one card can be used.
- Scanning a fingerprint and reading a card: The master device should be used for scanning a user's fingerprint or issuing a card. A 2.x device connected as the slave cannot scan a fingerprint or read a card.

Door

- Door: A 1.x device and a 2.x device cannot be used together for configuring the door. In other words, devices of different versions cannot be set for the entrance and exit devices.
- Zone: A 1.x device and a 2.x device cannot be used together for configuring a zone. In other words, a zone cannot be configured with devices of different versions.

Access control

- Full Access / No Access: A 2.x device uses the access control information of users in preference to full access/no access set for the device. If there is no access control information set for the device, access is possible with the user authentication information registered by default, and in order to control the access of users specifically, access control information must be set.

Device

- Device tree: A 2.x device is always displayed on the sublist of the BioStar Server. If the server mode is used, a 1.x device is displayed on the sublist of BioStar Server, and if the direct mode is used, it is displayed on the sublist of the device.
- Network tab: RS485 mode, which can be set for a 2.x device, is different from a 1.x device. The default value, host, and slave can be set as the RS485 mode for a 2.x device, and if the default value is set, one door can be configured with one device. Also, when a device whose Default Value is set for the RS485 mode is connected to the host device using a RS485 cable, it can also be registered as a slave device in the BioStar.
- Input/output tab: Device version 2.x only uses the input tab.
- Wiegand tab: Only the extension mode is supported for the Wiegand mode.
- MIFARE card CSN: Byte order of MIFARE card ID is different from a 1.x device. If **Byte Order** of 1.x devices is set to **MSB**, **Byte Order** of 2.x devices should be set to **LSB**. If **Byte Order** of 1.x devices is set to **LSB**, **Byte Order** of 2.x devices should be set to **MSB**.

Monitoring

- Arm/disarm: Arm/disarm cannot be used for a door or zone which is configured with a 2.x device.
- Uploading a log: A log can be uploaded using USB for a 2.x device.

02 Install the BioStar Software

Installing BioStar is a fairly simplistic process, provided that you address a few prerequisites before beginning the installation:

- First, you must select a PC that can remain running constantly to function as the BioStar server. The server will receive and store log data from connected devices in real time.
- Second, you must choose a type of database to use. The BioStar server supports either MySQL or MS SQL Server (including the scaled-down, free MS SQL Server Express). Regardless of which database you choose, you must have sufficient access rights and privileges to connect to the database and create new tables.
- Third, ensure that the PCs you will use for both server and client applications meet the minimum requirements listed in section 2.1.

The BioStar installation CD includes the BioStar installer. By default, the installer will install both the server and client applications with minimal input (see section 2.2). However, you may choose to install the server and client applications independently if you need to specify additional database options or desire to install the applications on separate PCs (see sections 2.3 and 2.4).

2.1 System Requirements

BioStar supports the following operating systems:

- Windows 10 (32bit or 64bit)
- Windows Server 2012 R2
- Windows 8 (32bit or 64bit)
- Windows 7 (32bit or 64bit)
- Windows Server 2008 R2
- Windows Vista

- Windows Server 2003

The minimum system requirements for installing and operating the BioStar software include the following:

- **CPU**: Intel Dual Core or similar processor, capable of processing speeds of 1.5GHz or faster
- **RAM**: 2GB
- **HDD**: 5GB

However, Suprema recommends the following hardware configuration for optimal performance:

- **CPU:** Intel Quad Core or similar processor, capable of processing speeds of 2GHz or faster
- **RAM**: 4GB
- **HDD**: 10GB

2.2 Run the BioStar Installer

You should run the BioStar installer when you desire to install both the server and client applications on the same PC and are willing to use the MS SQL Server Express database with default settings. You will be required to intervene in the express installation process only when MS SQL Server or a variation is already installed. In this case, you will be asked whether or not you wish to install MS SQL Server Express. If you choose not to install the express version, you will be required to provide the correct authentication details, as described in step 7 of section 2.3.

Attention: If you have installed a previous installation on the machine with BioStar installer, remove the old version before runninng the BioStar Installer.

Attention: Do not install BioStar 1 on a computer where BioStar 2 is installed. A problem in the performance of the program may occur.

2. Install the BioStar Software

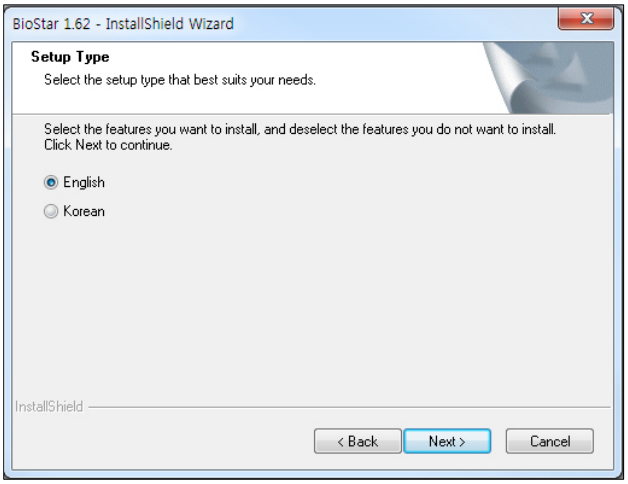
The installer will install the following components:

- BioStar server application
- Auxiliary libraries: OpenSSL and Microsoft Visual C++ Redistributable
- MS SQL Server 2012 Express
- BioStar client application
- BADB Conv (database migration tool)

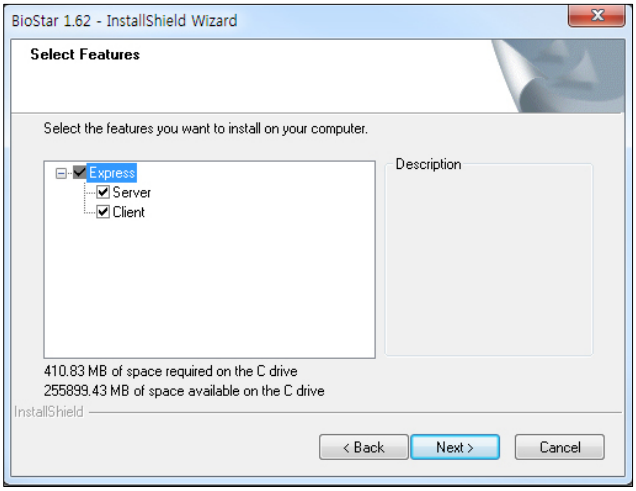
Before you run the BioStar installer, close all other open applications. If you have previously installed BioAdmin on the same machine, ensure that you stop the BioAdmin server before beginning the installation.

To run the installer:

1. Insert the BioStar installation CD into a compatible media drive.
2. Locate the installation directory and run *BioStar 1.93 Setup*.
3. Follow the on-screen prompts to begin the installation.
4. During the installation, you will be asked to select the language of your preference. Select a language, then click **Next** to proceed.



5. Make sure that both the Server and Client applications are selected in the **Select Features** dialog box, then click **Next** to proceed.



6. Follow the instructions on the screen to finish the installation.

2.3 Install the BioStar Server Application

If you do not choose to install the BioStar server and client applications together, you need to select only the application you would like to install at the Select Features dialog box during the installation of the Biostar Setup. After you ensure that your system meets the minimum requirements listed in section 2.1 and address the prerequisites mentioned in the introduction to this chapter, close all other open applications. If you have previously installed BioAdmin on the same machine, ensure that you stop the BioAdmin server before beginning the installation.

Attention: If you have installed a previous installation on the machine with BioStar installer, remove the old version before runninng the BioStar Installer.

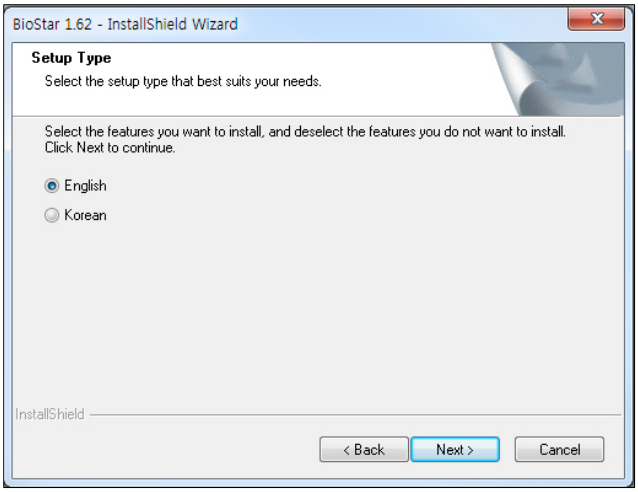
The installer includes the following components:

- BioStar server application
- Auxiliary libraries: OpenSSL and Microsoft Visual C++ Redistributable
- MS SQL Server 2012 Express
- BioStar client application
- BADB Conv (database migration tool)

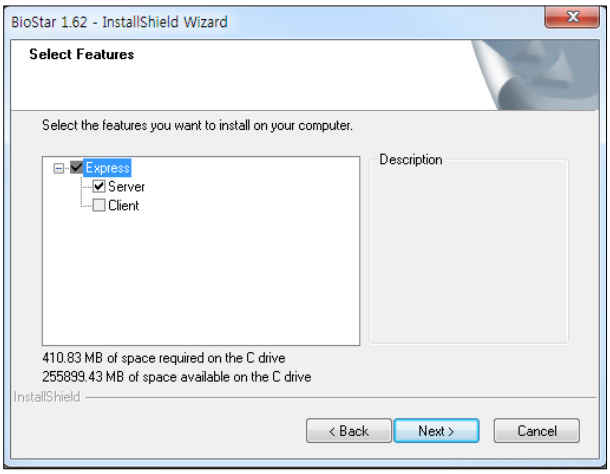
To install the BioStar server application:

1. Insert the BioStar installation CD into a compatible media drive.
2. Locate the installation directory and run *BioStar 1.93 Setup*.
3. Follow the on-screen prompts to begin the installation.

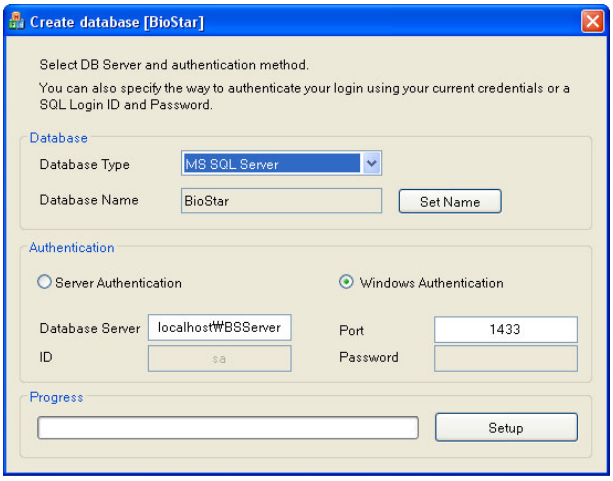
4. During the installation, you will be asked to select the language of your preference. Select a language, then click **Next** to proceed.



5. At the **Select Features** dialog box, click the Client checkbox to uncheck it and exclude the Biostar client application in the installation (both the server and slient applications are checked by default), then click **Next** to proceed.



6. Follow the instructions on the screen to finish the installation.
7. During the installation, you will be required to accept the OpenSSL license agreement and select a destination folder for the OpenSSL program files.
8. You will also be asked whether or not you wish to install the MS SQL Server 2012 Express edition. If you will use a pre-installed version of MS SQL Server, MySQL or Oracle, you may click **No** when this message appears. If you decide to use the express edition in this step, you can skip to step 10. The database setup process will be automated when you install the express edition.
9. When the **Create Database [BioStar]** dialog box appears, select a database type (MS SQL Server, MySQL or Oracle). The database server address and port numbers will be automatically populated, but you should verify that they are correct.



Note: The default name for the database is always "BioStar," to prevent unintentional installation of multiple databases on the same system or database server. The database name can be changed by editing the DBSetup.exe file. When patching the database server, you will have the option to manually select a datbase.

10. If you choose MS SQL Server, you must configure the authentication method as well (MySQL allows only server authentication):
    - **Server authentication**: this option uses login IDs and passwords to authenticate users that are created by and stored on the SQL Server. These credentials are not based on Windows user accounts. Users connecting via server authentication must provide their credentials every time that they connect.
    - **Windows authentication**: this option uses Windows users accounts for authentication. When users connect through a Windows user account, the SQL Server validates the account name and password using the Windows principal token in the operating system. The SQL Server does not ask for a password and does not independently validate user identification. Windows authentication is the default authentication mode for MS SQL Server.

Note: You must choose the authentication mode that is supported by the database. You must also provide the proper credentials to create new tables in the database.

11. Click **Setup** to create the SQL database.
12. When the SQL database setup is complete, click **Finish**.
13. The setup program will perform a few remaining processes before the server installation is complete. Click **Finish**.

2.3.1 Configure the MySQL Database

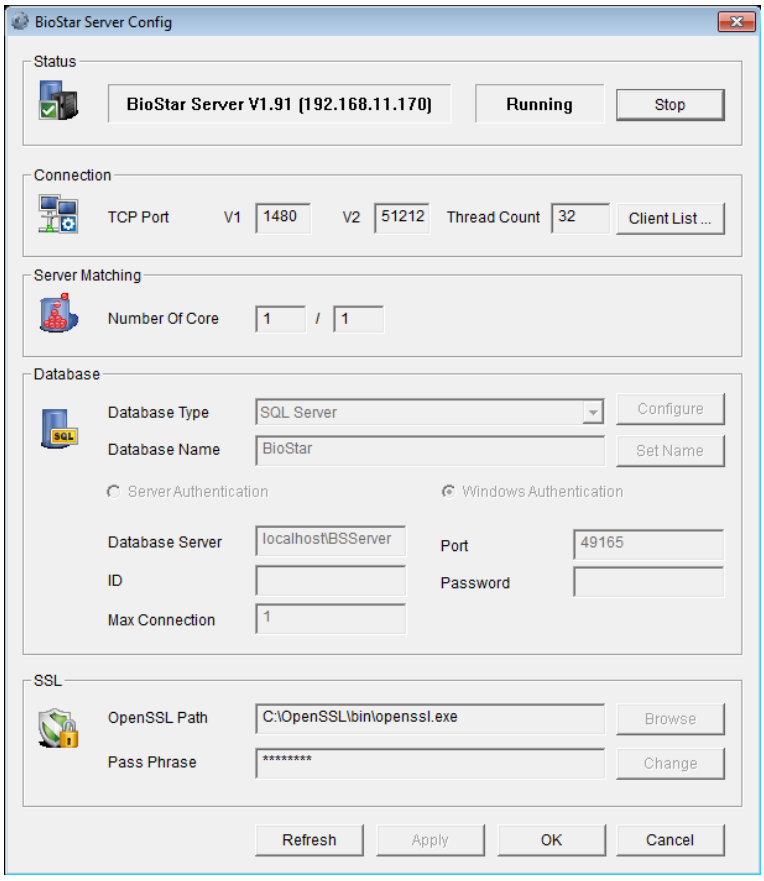
BioStar cannot use the MySQL database if the maximum packet size is less than 16MB. To configure the maximum packet size n MySQL server, locate and open a configuration file for the MySQL server ("my.ini" for a Windows system or "my.cnf" for a Linux system). Under [mysqld], add or edit the packet size to 16M or bigger (for example:

max_allowed_packet=16M). After you have changed and saved the file, restart the BioStar Server for the changes to take effect.

2.3.2 Configure the BioStar Server

In some cases, you may require manual configuration of the BioStar server. If you are having trouble connecting to the server from the client application, for example, you may need to alter your server settings. In addition, you must stop and restart the server application to apply any changes you have made to server configurations or database settings.

On desktop, click BioStar Server Config to start BioStar Server setting program. Or, in Windows, Start > All programs > BioStar 1.93 > Server Service > BioStar Server Config



The server configuration utility allows you to monitor and control the following:

- **Status**: view and modify the current status of the BioStar server (*Stopped* or *Started*). You can stop and start the server by clicking the **Start** or **Stop** button on the right.
- **Connection**: view and modify the details for the connection between the server and devices.

  - **TCP Port**: enter the port that devices and client applications use to connect to the server. You should use a port that is not shared with any other software applications. Most devices supporting BioStar 1 use 1480 port as a default, and BioStation A2, BioStation 2 and BioStation L2 use 51212 port as a default.
  - **Thread Count**: enter the maximum thread count that the BioStar server can create. You can enter any number between 32 and 512; however, keep in mind a larger thread count will consume more system resources.
  - **Client List**: click this button to view a list of devices that are connected to the BioStar server. The list shows the IP address of each device and whether or not a SSL certificate has been issued to the device. You can issue or remove SSL certificates directly from the utility.
- **Server Matching**: The function of the matcher used at the time of server matching is improved according to the number of CPU cores in the system. Therefore, a faster server matching speed can be expected as the number of cores used by the matcher becomes larger. The following setting is supported at the Server Matching item in the BioStar Server Config.
  - **Number Of Core**: means the number of cores used by the matcher and the default number is 2.
- **Database**: view and modify database settings. For more information about how to alter these settings, see the procedure for setting up the BioStar server in section 2.3.
  - **Max Connection**: specify the maximum number of connections between the server and the database. In most cases, the default value (1) is appropriate.
- **SSL**: view or modify the settings for OpenSSL. Click Browse to locate the path for the OpenSSL application or click Change to change the pass phrase.

2.4 Install the BioStar Client Application

If you do not choose to install the BioStar server and client applications together, you need to select only the application you would like to install at the **Select Features** dialog box during the installation of the Biostar Setup.

Before you install the BioStar client application, close all other running applications.

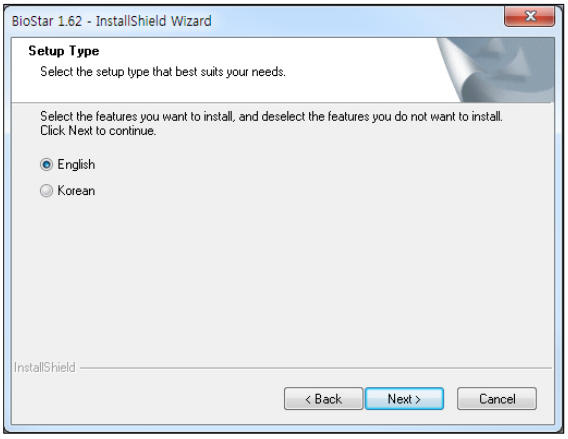
The installer includes the following components:

- BioStar server application
- Auxiliary libraries: OpenSSL and Microsoft Visual C++ Redistributable
- MS SQL Server 2012 Express
- BioStar client application
- BADB Conv (database migration tool)

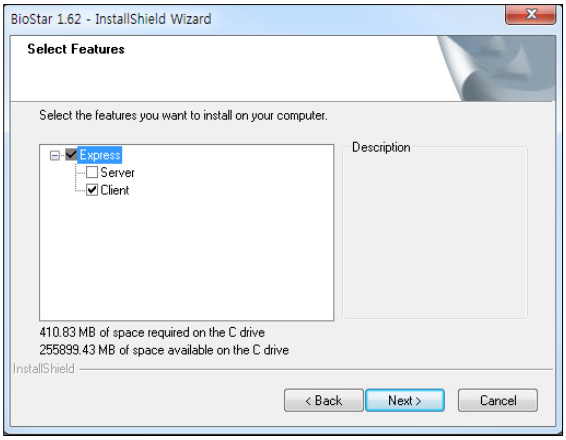
To install BioStar client application:

1. Insert the BioStar installation CD into a compatible media drive.
2. Run *BioStar 1.93 Setup* to launch the installation wizard.

3. Follow the on-screen prompts to install the BioStar Client.
4. During the installation, you will be asked to select the language of your preference. Select a language, then click **Next** to proceed.



5. At the **Select Features** dialog box, click the Server checkbox to uncheck it and exclude the Biostar server application in the installation (both the server and client applications are checked by default), then click **Next** to proceed.



6. Follow the instructions on the screen to finish the installation.

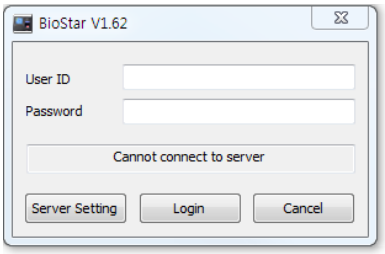
Attention: BioStar versions 1.3 and higher include a USB driver, which enables the connection of BioStation in Windows 7. This driver is not compatible with a previous version of BioStar. If a previous version of BioStar is used, install the correct USB driver.

2.4.1 Log in to BioStar for the First Time

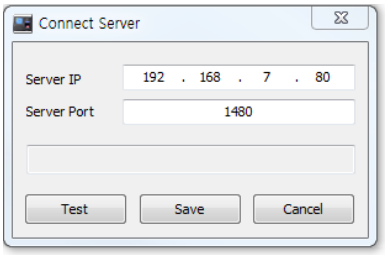
If you restarted the system after installation, the BioStar server should run automatically in the background. If you have not restarted the system, you may be required to manually connect to the server before proceeding (see section 2.3.2). When logging in to BioStar for the first time, you will be prompted to create an administrator account.

To log in for the first time:

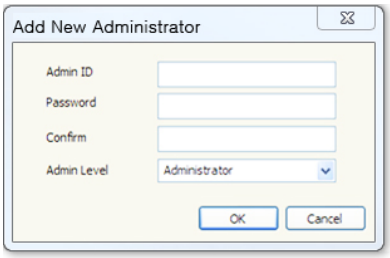
1. Launch the BioStar program. If BioStar successfully connects to the server, the **Add New Administrator** dialog box will open. In this case, skip to step 6. If BioStar cannot connect to the server, the **Login** dialog box will open and display the message "Cannot connect to server."



2. Click **Server Setting**. This will open the **Connect Server** dialog box.



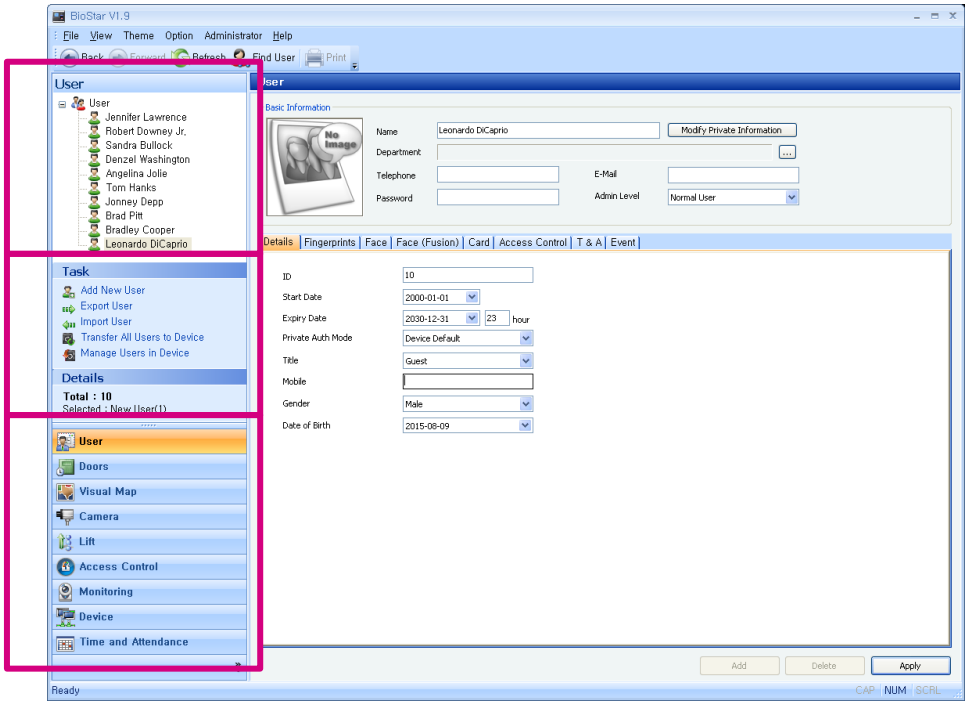
3. Enter the IP address and port number of the BioStar server.
4. Click **Test** to verify the connection.
5. Click **Save** to store the connection settings. This will open the **Add New Administrator** dialog box.



6. Enter an Admin ID and password, confirm the password, and choose an administration level from the drop-down level.
7. Click **OK**. This will return you to the **Login** dialog box.
8. Enter a User ID and password and click **Login**.

2.5 BioStar Interface

BioStar is composed of various interface elements. Each element uses a standard name, please check names of each element before you read this manual.



Each element is named as what is displayed in the title. For example, it is called User window, Customize dialog box, Additional Infomation tab, Basic Information area.

2.6 Customize the BioStar Interface

You do not have to make any changes to the interface to use the BioStar system—the default settings are sufficient for setup and operation. However, BioStar allows you to customize various settings to control the appearance and functionality of the interface.

2.6.1 Change the Theme

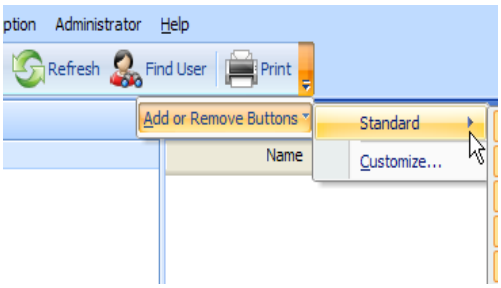
The BioStar interface includes two preset themes based on MS Office styles:

- Office 2003
- Office 2007

To change the theme, click **Theme** from the menu bar and select a theme.

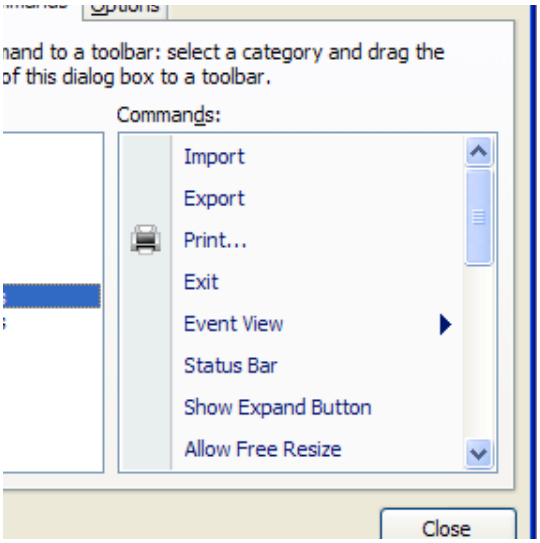
2.6.2 Customize the Toolbar

The BioStar interface includes a standard toolbar near the top left of the screen. Standard toolbar buttons provide functions similar to a typical web browser: Back, Forward, Refresh, Find User (search), and Print.



To customize the toolbar:

1. Click the drop-down arrow at the right of the toolbar.
2. Click **Add or Remove Buttons > Customize**. This will open the **Customize** dialog box.
3. Click the Commands tab.
4. Click *All Commands* to display a list of available buttons.



5. Drag a command to the toolbar. This will add a new button for the command.

2.6.3 Change Event Views

BioStar allows you to change the default period of events to show in the Event tab for users or doors and zones. You can set the interface to show event details for 1 day, 3 days, or 1 week by default.

To change the event view:

1. From the menu bar, click **View** > **Event View**.
2. Click type of event view to change (*User* or *Doors/Zone*).
3. Click a default event period (*1 day*, *3 day*, or *7 day*).

2.6.4 Change Event Views

The fonts installed on the system can be used in BioStar in order to support various languages. After changing the font, restart BioStar.

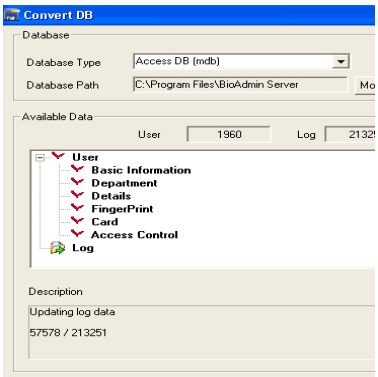
2.7 Migrate a Database from BioAdmin to BioStar

The BioStar installation program includes a database migration tool called *BADB Conv*. This tool allows you to migrate an existing BioAdmin database to your new BioStar system.

When migrating a database, any identical information that exists in the BioStar database will be overwritten. For example, if you have added a user to BioStar that previously existed in BioAdmin, the user data will be overwritten with the information from the BioAdmin database. For this reason, you should migrate your old database to BioStar before creating new user accounts.

To migrate your information from BioAdmin to BioStar:

1. Locate and run the migration program, *BADBConv.exe*. The location of this program is Window's Start > All Programs > BioStar 1.93 > Server Service > BADBConv.
2. Click **Yes** to acknowledge the warning dialogue that appears to remind you that identical information in BioStar will be overwritten.
3. Click **Start** to begin the migration. When the process is complete, the **Convert DB** dialog box will show the types of data that have been migrated.



4. Click **Close** to exit the migration tool.

03 Setup the BioStar System

This section describes how to add administrator accounts, devices, doors, zones, departments, users, and access groups and setup time and attendance within the BioStar software. This administrator's guide does not cover procedures for installing physical components, wiring doors and devices, or connecting devices to networks. For more information about hardware installation and physical configuration of your access control system, please refer to the installation guides that accompany your access control devices.

3.1 Create Administrative Accounts

Before adding users, it is a good idea to add and configure accounts for system administrators and operators. It is also useful to understand some general concepts regarding administration of the BioStar system.

3.1.1 Administrative Levels

BioStar allows for multiple levels of administration, operation, and interaction with the system. Each administrative level has varying degrees of privileges and access to the system menus (User, Doors, Visual Map, Access Control, Monitoring, Devices, and Time & Attendance). The BioStar system includes three preset administrator levels in addition to custom administrator levels:

- Administrator
- Operator
- Manager
- Custom administrator levels

Administrators are capable of adding and configuring devices, users, doors, zones, and access groups. They also can manage time and attendance functions, including setting up time categories, daily schedules, shifts, holiday rules, and leave periods, as well as creating, modifying, and viewing time and attendance reports. In addition, administrators can create custom administrator levels that are granted various privileges for the BioStar system menus.

Operators can monitor and manage the BioStar system via a remote client terminal. Operators have the same privileges with administrators, other than the privileges to create and delete other administrator or operator accounts. Like administrators, operators are capable of adding and configuring devices, users, doors, zones, and access groups. They also can manage time and attendance functions, including setting up time categories, daily schedules, shifts, holiday rules, and leave periods, as well as creating, modifying, and viewing time and attendance reports.

Managers have privileges to read all information in the menus. However, they cannot create, modify, or delete anything in the menus. Depending on your organization's requirements, the capability to view events may be useful for other management purposes.

The custom administrator level can be assigned full or limited privileges on the seven menus. On each menu, you can assign one of three privileges: All Rights, Modify, or Read. Depending on your organization's requirements, the BioStar system can be managed more effectively by adding custom administrator levels.

A typical setup will consist of one administrator (or more, depending on the size of your organization) who has full access to the system. Below the administrator level, several operators may perform various functions, such as remotely controlling doors and locks, adding users, registering fingerprints, issuing access cards, adding access groups, defining timezones, and configuring alarm events.

3.1.2 Add and Customize Administrative Accounts

By default, BioStar includes one administrator account, which is added when you install the software (see section 2.3). You may choose to use this account as the sole administrator and grant operator privileges to all other users who will manage the system or you may choose to add multiple administrators to the system.

3.1.2.1 Add an administrative account

To add an administrative account:

1. From the menu bar, click **Administrator** > **Admin Account** to open the **Admin Account List** dialog box.
2. Click **Add New Administrator**.
3. In the **Add New Administrator** dialog box, enter an Admin ID and password.
4. Confirm the password by retyping it and select an Admin Level from the drop-down list:

- **Administrator**: all privileges.
- **Operator**: all privileges, other than creating or deleting administrator or operator accounts.
- **Manager**: privilege to read all information.

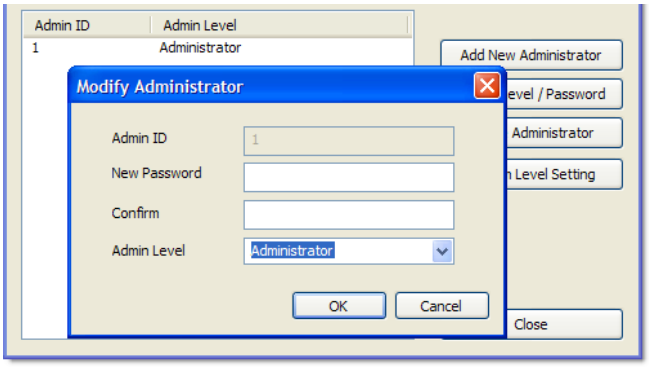
5. Click **OK**.

3.1.2.2 Change an administrative account level or password

If you accidentally set the wrong level for an administrative account or need to change or reset a password, you can do so from the Administrator menu.

To change an administrative level or password:

1. From the menu bar, click **Administrator > Admin Account** to open the **Admin Account List** dialog box.
2. Click an admin account in the list on the left side of the dialog box.
3. Click **Modify Level/Password**. This will open the **Modify Administrator** dialog box.



4. Edit the account information as required:
   - To change the administrative level, choose a new level from the drop-down list.
   - To change the password, type a new password in both the New Password and Confirm boxes.
5. Click **OK** to save the changes.

3.1.2.3 Create a custom administration level

If you need to define a specific administrator role with particular privileges, you can add a custom administrator level. You can allow full or limited access to any of BioStar's seven menus for the custom administrator level: User, Doors, Visual Map, Access Control, Monitoring, Devices, and Time & Attendance.

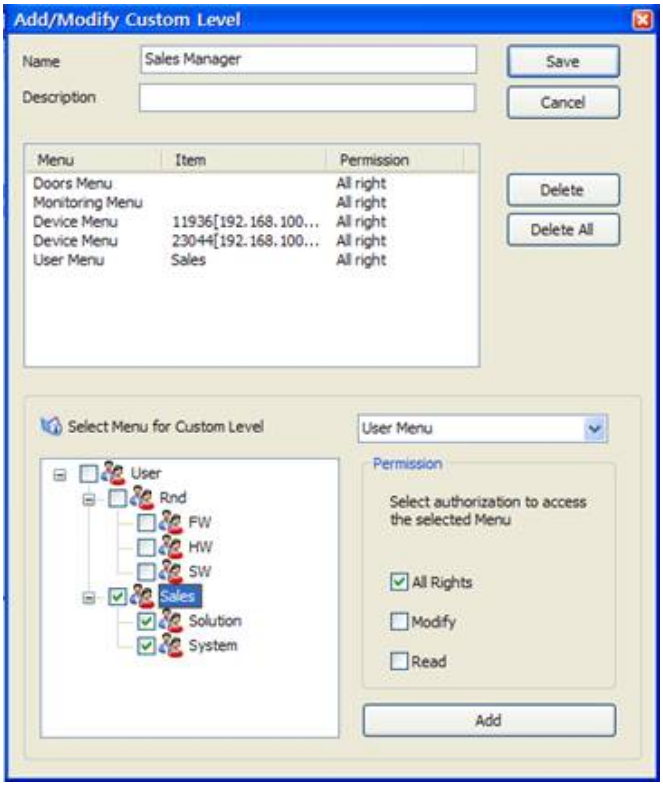
The custom administrator level can be assigned privileges for specific users and devices. A custom administrator will have the privileges you assign (All Rights, Modify, or Read) only for those users or devices that you specify and will not be

allowed to view or modify other users or devices. While you are creating a custom administrator level, in the User menu, you can grant privileges for users in a department and its sub departments. However, ensure that you do not select individual users, but rather the first-level or second-level departments they belong to.

In the Device menu, you can grant privileges for specific devices. If a device has a slave device connected, the privileges for the host device will also apply to the slave device. Users and devices that are not selected in the User and Device menus will not appear in the Doors, Visual Map, Access Control, Monitoring, and Time and Attendance menus. If a door or zone is associated with devices that are not granted privileges, the door or zone will not appear in the Door menu.

To create a custom administrator level:

1. From the menu bar, click **Administrator > Admin Account** to open the **Admin Account List** dialog box.
2. Click **Custom Level Setting**.
3. From the **Custom Level List** dialog box, click **Add Custom Level**. This will open the **Add/Modify Custom Level** dialog box.



4. Type a name for the custom level in the Name field.
5. If desired, add an additional description in the Description field.
6. Select a menu from the drop-down list.

7. When selecting the User Menu or Device Menu, select users or devices to grant access privileges by clicking the checkboxes in the users or devices list.
8. Select a permission level (All Rights, Modify, or Read) by clicking the checkbox next to an option.
9. Click **Add** to include the permission in the custom level.
10. Repeat steps 6-9 as necessary to add other permissions.
11. When you are finished customizing the level, click **Save**.

You can now create new administrative accounts with any of the custom administrator levels you have created.

3.2 Setup Devices

This section describes how to use BioStar's device wizard to search for and add new devices, as well as how to add 3rd party RF devices. In addition, the procedures that follow describe basic configuration of devices within the BioStar system. For more information about configuring devices, see sections 3.10.3 and 5.1.

3.2.1 Search for and Add Devices

BioStar includes a handy wizard for finding and adding devices. Before starting a search for new devices, verify the device connections. If you have multiple devices to add, it may be helpful to prepare a list of device locations, IDs, and IP addresses prior to adding them.

To search for devices and add them to the BioStar system:

1. Click **Device** in the shortcut pane.
2. In the Task pane, click *Add Device*.
3. When the wizard appears, click the option button next to a connection type:
   - **LAN**: Choose this option to search for devices connected via Ethernet or Wireless LAN.
   - **Serial**: Choose this option to search for devices connected to a client PC via RS485 and RS232 or slave devices connected via RS485 to another device that is connected to a client PC (see section 3.2.2).
   - **USB Device**: Choose this option to search for devices connected via USB ports.
   - **Virtual USB Device**: choose this option to search for virtual devices that you have added to a USB drive.

Attention: BioStar versions 1.3 and higher include a USB driver, which enables the connection of BioStation in Windows 7. This driver is not compatible with a previous version of BioStar. If a previous version of BioStar is used, install the correct USB driver.

4. Click **Next**.
5. For USB or Virtual USB searches, skip to step 7. If you are searching for devices connected via LAN or serial ports, set advanced search criteria:
   - **LAN**: Select whether to search for devices using TCP or UDP protocols. When you select TCP, you can specify an IP address range, the type of device you are searching for (BioStation/X-Station/BioStation T2/FaceStation: 1470, BioEntry Plus/BioEntry W/BioLite Net/Xpass/Xpass S2: 1471, BioStation A2/BioStation 2/BioStation L2/BioEntry W2: 51212 or Custom: enter manually), and the port to search with. If you select UDP, you can search for devices only in the same subnet.
   - **Serial**: Specify a COM port (or select *All port*) and a baud rate. You can connect up to 31 devices per COM port via RS485. If the RS485 cable is too long, the signal may be weakened. In this case, you should install a terminating resistance at both ends of the bus by turning on the Dip Switch on your device for normal signal transmission. On the other hand, if the cable is too short, the resistance may interrupt signal transmission. Therefore, by considering the length of the cable and the signal status, select whether to turn on or off the terminating resistance switch.

Note: The RS485 mode setting is different between a 1.x device and a 2.x device. **Disable**, **Host**, **Slave** and **PC Connection** can be used for a 1.x device, and **Default**, **Host**, and **Slave** can be used for a 2.x device.

If **Default** is set as the RS485 mode for a 2.x device, one door can be configured with one device. In order to configure one door with two devices such as the Anti-passback zone, the RS485 mode should be changed to **Host** or **Slave**.

Also, when a device whose **Default** is set as the RS485 mode is connected to the host device using a RS485 cable, it can be searched as a slave device in the BioStar.

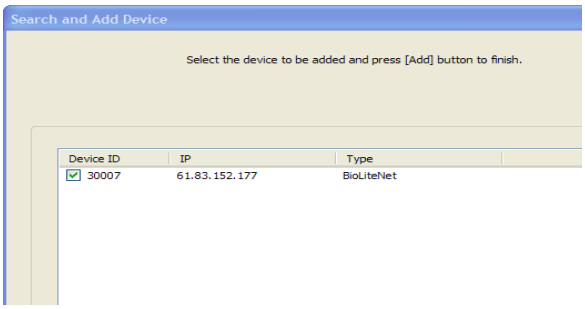
6. Click **Next**.
7. When BioStar completes the search, you can specify network settings as described below. Click a device name in the list on the left and then configure the settings as required:

Note: If you change the network settings for a device at this point, the device will be removed from the device list. To add the device in the following steps, you must search for the device again.

You need not and should not add devices with server mode. The devices will connect to the server by themselves, and will be listed under the BioStar Server on the **Device Tree** dialog box. If you are trying to add devices with server mode, the process will fail.

- **DHCP or Static IP:** If you choose to use the DHCP option, the device will automatically acquire network settings from the DHCP server. If you do not use DHCP, you must configure the network settings manually.
- **Direct connection**: This is the default connection option. With this option, the BioStar client will connect directly to the device. If you choose this type of connection, the BioStar client must be running to retrieve the log records from the device.
- **Server connection**: If you choose this option, the device will automatically connect to the BioStar server. If you configure the server IP address and port correctly, log records from the device will be gathered at the server, regardless of whether or not the BioStar client is online. This option may also be useful if your network configuration requires you to connect devices with private IP addresses (for example, over a WAN) to a server with a public IP address. This option also provides SSL encryption for BioStation devices.

8. Click **Next**.
9. Select the device or devices to add by clicking the checkboxes next to the device IDs.



10. Click **Add** to add the devices to the BioStar system.
11. Close the confirmation message that appears and click **Finish** to exit the wizard.

Note: You can manage devices by group by creating a tree hierarchy of named groups and assigning devices into one of the groups. Groups are created by right-clicking on the desired position in the device tree and selecting **Add Group**. You can drag and drop devices between different locations of groups. Groups can be nested four levels deep and a pair of host-slave devices moves together.

3.2.2 Search for and Add Slave Devices

A distinctive feature of BioStar is that it supports host and slave devices in RS485 networks. With this feature, only the host device must be connected to a PC via the LAN. The network can then be easily expanded by adding slave devices via RS485 connections.

This feature also allows for controlling elevator (lift) access with BioEntry Plus, Xpass and Xpass S2 devices that are connected to LIFT I/O devices.

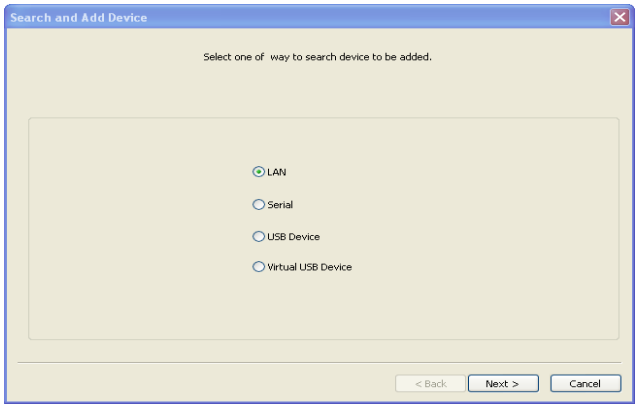
If your configuration includes slave devices, you must perform an additional search to locate and add those devices.

First, configure the host device:

1. Search for and add the host device as described in section 3.2.1.
2. Click **Device** in the shortcut pane.
3. In the navigation pane, click the host device.
4. In the device pane, click the Network tab.
5. Change the RS485 serial setting by selecting *Host* from the Mode drop-down list.
6. Click **Apply** to save the change.

Next, search for and add slave devices:

1. In the navigation pane, right-click the host device and click **Add Device (Serial)**. This will open the **Search and Add Device** dialog box.



2. Click **Next** to begin the search.
3. When BioStar completes the search, click **Next**.
4. Select the device or devices to add by clicking the checkboxes next to the device IDs.
5. Click **Add** to add the device
6. Close the confirmation message that appears and click **Finish** to exit the wizard.
7. In the navigation pane, click the slave device.
8. In the device pane, click the Network tab.
9. Change the RS485 serial setting by selecting *Slave* from the Mode drop-down list.
10. Click **Apply** to save the change.

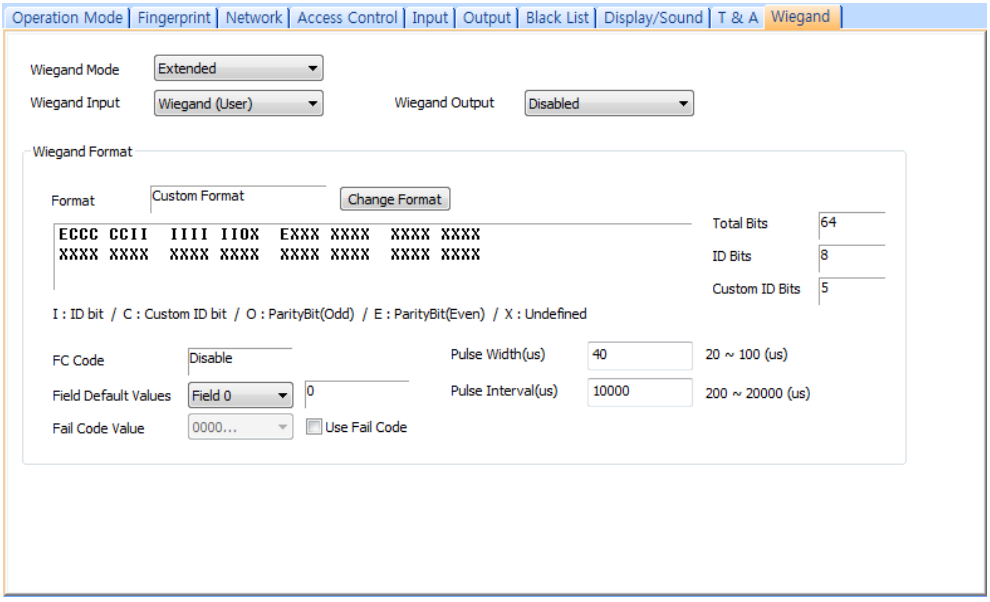
3.2.3 Add an RF Device

Prior to BioStar 1.2, third-party RF devices connected to Suprema devices (BioStation, BioEntry Plus, BioEntry W, and BioLite Net devices), operated only as physical extensions to

the Suprema devices. As of BioStar 1.2, third-party RF devices connected to Suprema devices function independently and can be associated with doors and included in zones.

To add an RF device:

1. Connect the RF device to a Suprema device.
2. Ensure that the Suprema device is added to the BioStar system (see section 3.2.1).
3. Click **Device** in the shortcut pane.
4. In the navigation pane, click the Suprema device name.
5. Click the Wiegand tab and specify Wiegand settings as described below.



   b. Select **Extended** in the Wiegand Mode drop-down list.
   c. Select **Wiegand (Card)** in the Wiegand Input drop-down list.
   d. Click **Apply** at the bottom of the pane.
6. In the navigation pane, right-click the BioStation device name and then click *Add RF Device*.

Note: For more information about using your third-party RF device, consult the user guidance for the RF device. The Wiegand format must be configured properly to ensure compatibility with third-party RF devices.

3.2.4 Connect a Device via Wireless LAN

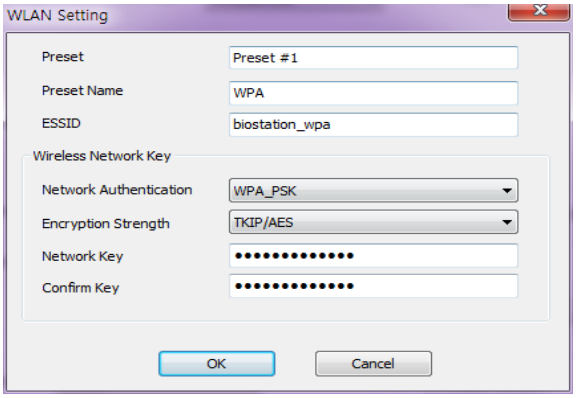
Certain BioStation devices (BSTW-OC, BSTW-TC, BSRW-OC, BSRW-TC) and BioStation T2, FaceStation, BioStation A2, BioStation 2 support wireless LAN connections.

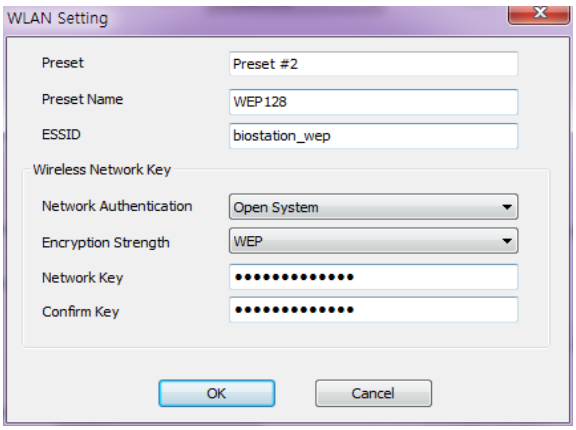
To configure the settings for a wireless LAN connection:

1. Click **Device** in the shortcut pane.

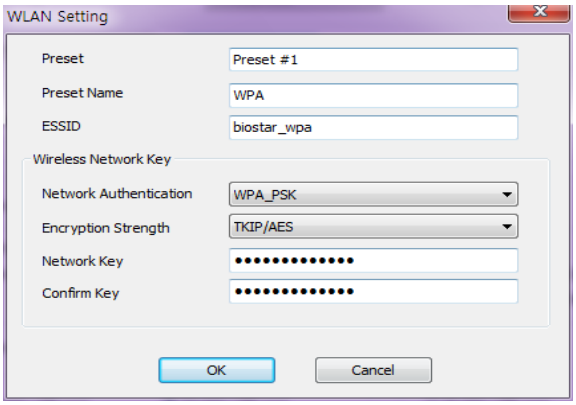
2. Click a device name in the navigation pane.
3. Click the Network tab in the Device pane.
4. Select "Wireless LAN" in the Lan Type drop-down list.
5. Select one of the preset configurations in the WLAN section (*Preset #1 ~ Preset #4*).
6. Click **Change Setting** in the WLAN section. If you choose to use 'Preset #1 or #2, the following figures will appear.

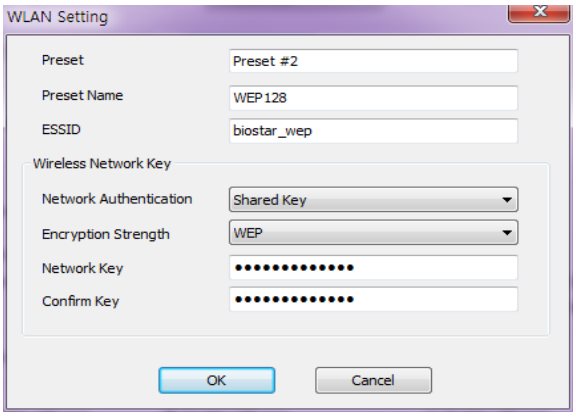
[Wireless LAN-supported BioStation models]





[BioStation A2, BioStation 2, BioStation T2 and FaceStation]





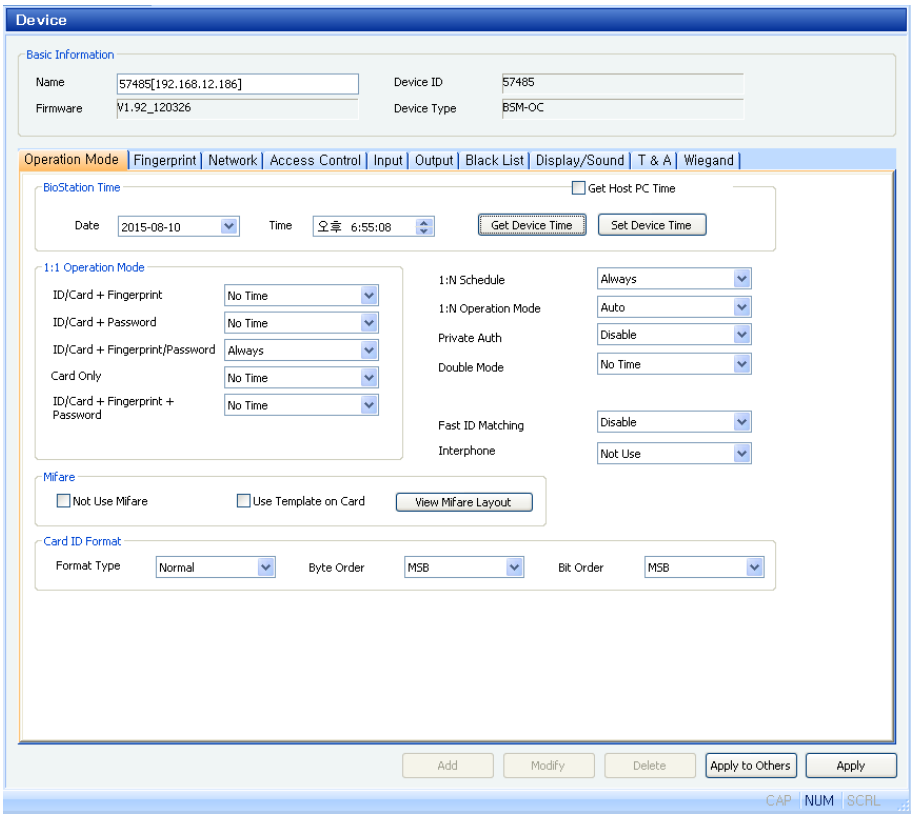
7. Optional: If you choose to configure your own wireless LAN by selecting Preset #3 or #4, then specify the following options.
   - **Preset Name**: Enter a name for the wireless LAN that the device will be connected to.
   - **ESSID**: Enter the unique ID of the access point.
   - **Network Authentication**: Select a network authentication mode from the drop-down list (*Open System*, *Shared Key*, or *WPA-PSK*). The authentication mode must be the same for the device and the access point.
   - **Encryption Strength**: Select an encryption strength from the drop-down list (available options depend on network authentication setting).
   - **Network Key: E**nter the network key. '_suprema_wpa_' is a pre-defined value for Preset #1 networks (biostation_wpa, biostar_wpa), and '_suprema_wep_' is for Preset #2 networks (biostation_wep, biostar_wep).
   - **Confirm Key:** re-enter the network key.
8. Click **OK** to save your changes.

3.2.5 Configure a BioStation Device

This section provides an overview of configuring BioStation devices to work with the BioStar software. For more information, refer to the installation guides that accompany your devices.

To configure a BioStation device:

1. Click **Device** in the shortcut pane.
2. Double-click a BioStation device name in the navigation pane. This will open a Device pane similar to the one below:



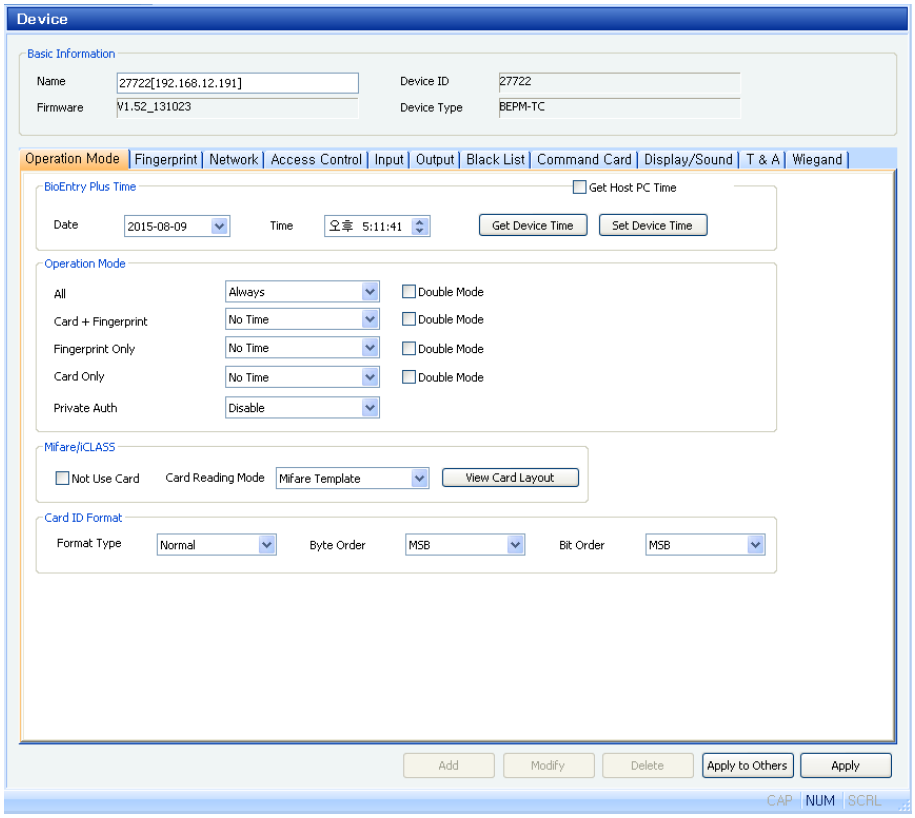
3. Configure device information on the following tabs. For an explanation of device settings, please see section 5.1.1.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
   - **Fingerprint:** Use this tab to specify security, quality, matching, and timeout settings for fingerprint recognition.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
   - **Input**: Use this tab to add, modify, or delete input settings for the device.
   - **Output**: Use this tab to add, modify, or delete output settings for the device.
   - **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
   - **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
   - **T&A:** Use this tab to configure time and attendance settings.
   - **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.
4. When you are finished configuring the device, click **Apply** to save your changes.

5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.6 Configure a BioEntry Plus or BioEntry W Device

To configure a BioEntry Plus or BioEntry W device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.2.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC, adjust settings for operation modes, and adjust options for fingerprint recognition.
   - **Fingerprint**: Use this tab to specify security, quality, matching, and timeout settings for fingerprint recognition.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control**: Use this tab to specify entrance limits, access groups, and time and attendance mode settings.
   - **Input**: Use this tab to add or modify inputs to the device.
   - **Output**: Use this tab to add or modify outputs from the device.

- **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
- **Command Card**: Use this tab to issue command cards that can control BioEntry Plus or BioEntry W devices. For more information about issuing command cards, see section 3.2.6.1.
- **Display/Sound**: Use this tab to configure LED & Buzzer settings according to the event or status.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.1.16.

4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.6.1 Issue command cards

Command cards allow you to enroll and delete users directly from a BioEntry Plus or BioEntry W device. For more information about enrolling users via command cards, see section 3.6.2.3. For more information about delete an individual or all users via command cards, see section 4.5.1.1 and 4.5.1.2.

To issue command cards:

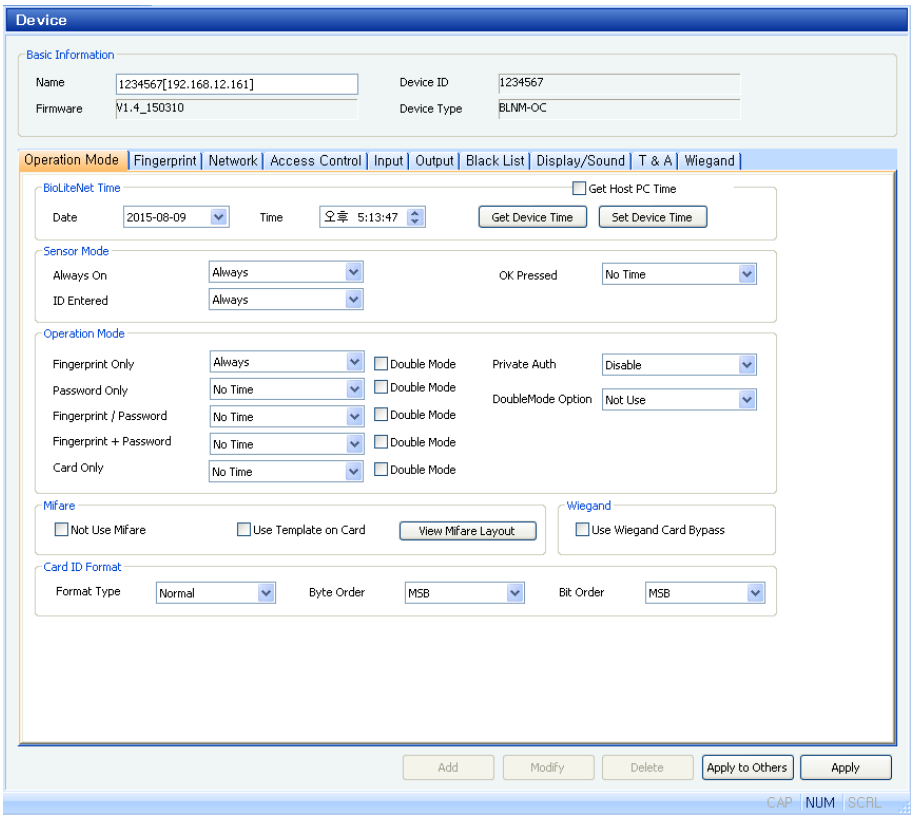
1. Click **Device** in the shortcut pane.
2. In the navigation pane, click the name of a BioEntry Plus or BioEntry W device.
3. Click the Command Card tab in the Device pane.

   Click **Read Card**.
4. Place a command card on the device.
5. Select a command type from the drop-down list.
6. If desired, set the command card to require administrator authentication by clicking the checkbox next to the option.
7. Click **Add**.

3.2.7 Configure a BioLite Net Device

To configure a BioLite Net device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



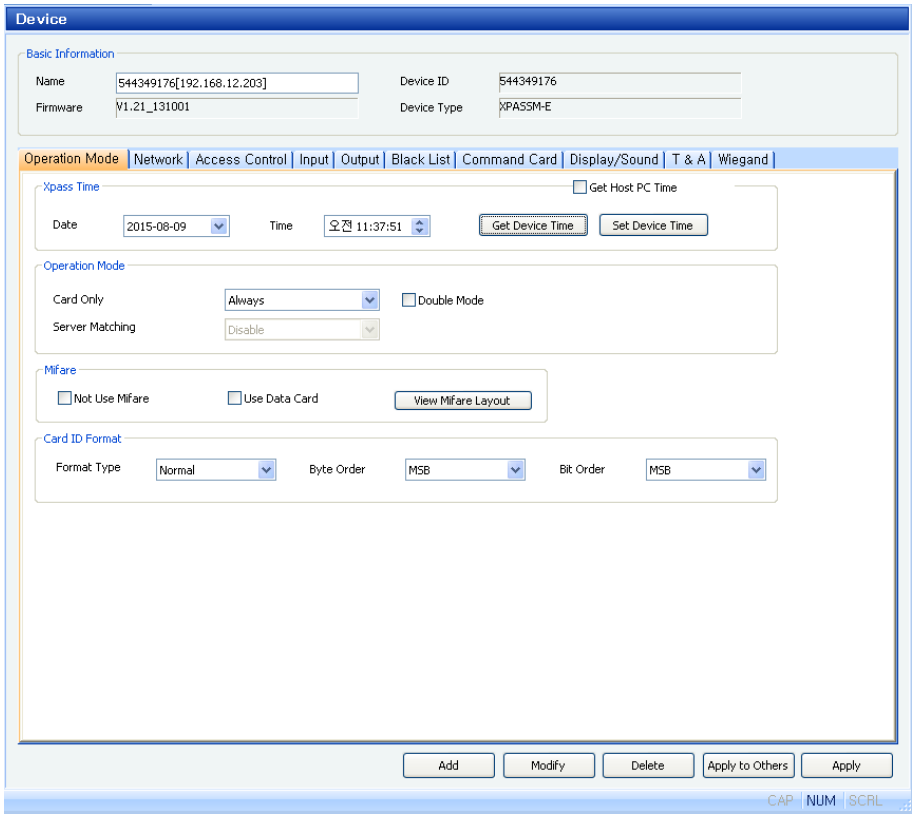
3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.3.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC, adjust settings for operation modes, and adjust options for fingerprint recognition.
   - **Fingerprint**: Use this tab to specify security, quality, matching, and timeout settings for fingerprint recognition.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control**: Use this tab to specify entrance limits and access groups.
   - **Input**: Use this tab to add or modify inputs to the device.
   - **Output**: Use this tab to add or modify outputs from the device.
   - **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
   - **Display/Sound**: Use this tab to configure LED & Buzzer according to the event or status.
   - **T&A:** Use this tab to configure time and attendance settings.
   - **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.
4. When you are finished configuring the device, click **Apply** to save your changes.

5. To apply the same settings to other devices, click **Apply to Others**, select other devices from the **Device Tree** dialog box, and click **Apply**.

3.2.8 Configure an Xpass or Xpass S2 Device

To configure an Xpass or Xpass S2 device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.4 (Xpass) or 5.1.5 (Xpass S2).
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC, adjust settings for operation modes, and adjust settings for card ID formats. Xpass S2 device do not support the Mifare template cards.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control**: Use this tab to specify entrance limits and access groups.
   - **Input**: Use this tab to add or modify inputs to the device.
   - **Output**: Use this tab to add or modify outputs from the device.
   - **Command Card**: Use this tab to issue command cards that can control Xpass or Xpass S2 devices. For more information about issuing command cards, see section 3.2.8.1.

- **Display/Sound**: Use this tab to configure LED & Buzzer according to the event or status.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.

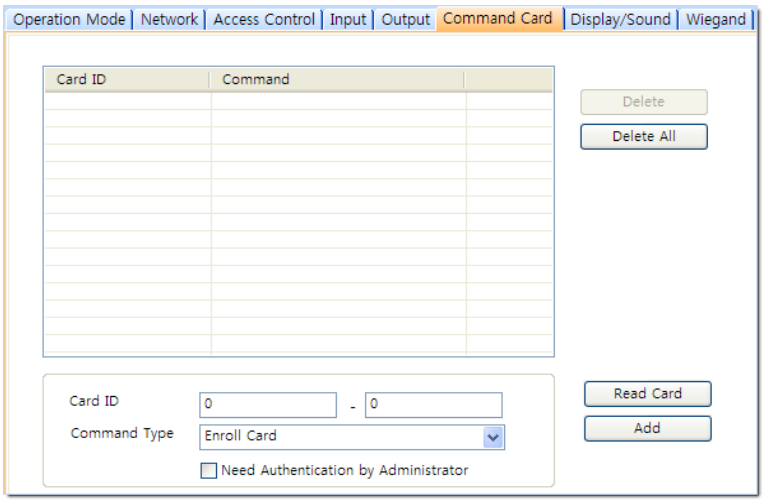
4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others**, select other devices from the **Device Tree** dialog box, and click **Apply**.

3.2.8.1 Issue command cards

Command cards allow you to enroll and delete users directly from an Xpass or Xpass S2 devices. For more information about enrolling users via command cards, see section 3.6.2.3. For more information about deleting an individual or all users via command cards, see section 4.5.1.1 and 4.5.1.2.

To issue command cards:

1. Click **Device** in the shortcut pane.
2. In the navigation pane, click the name of an Xpass device.
3. Click the Command Card tab in the Device pane.



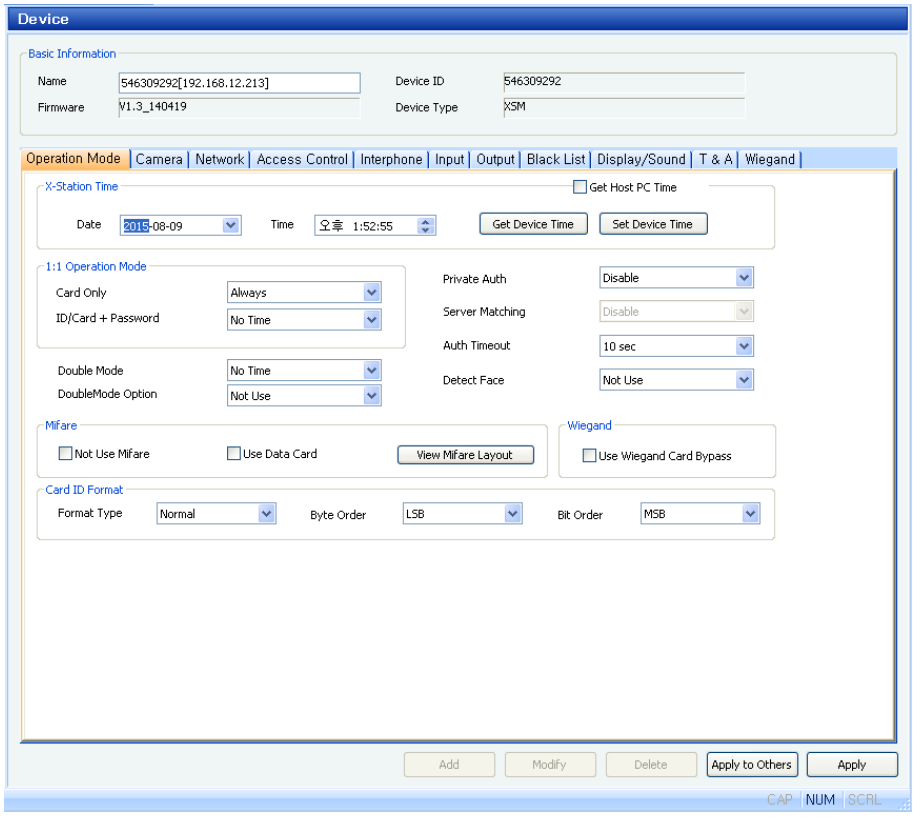
4. Click **Read Card**.
5. Place a command card on the device.
6. Select a command type from the drop-down list.
7. If desired, set the command card to require administrator authentication by clicking the checkbox next to the option.
8. Click **Add**.

3.2.9 Configure an X-Station Device

To configure an X-Station device:

1. Click **Device** in the shortcut pane.

2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.7.

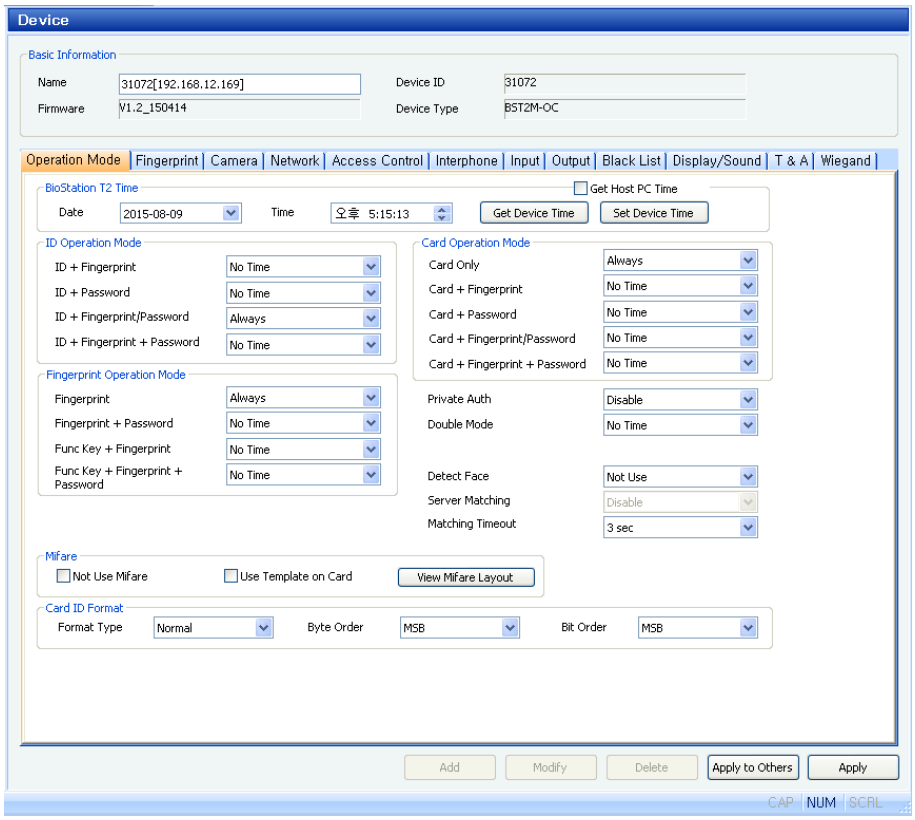
- **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
- **Camera**: Use this tab to assign events, by timezone, that can be performed via the camera and the face detection feature.
- **Network**: Use this tab to specify settings for LAN or serial connections.
- **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
- **Input**: Use this tab to add, modify, or delete input settings for the device.
- **Output**: Use this tab to add, modify, or delete output settings for the device.
- **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
- **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
- **T&A:** Use this tab to configure time and attendance settings.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.

4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.10 Configure a BioStation T2 Device

To configure a BioStation T2 device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.7.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
   - **Fingerprint:** Use this tab to specify security, quality, matching, and timeout settings for fingerprint recognition.
   - **Camera**: Use this tab to assign events, by timezone, that can be performed via the camera and the face detection feature.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.

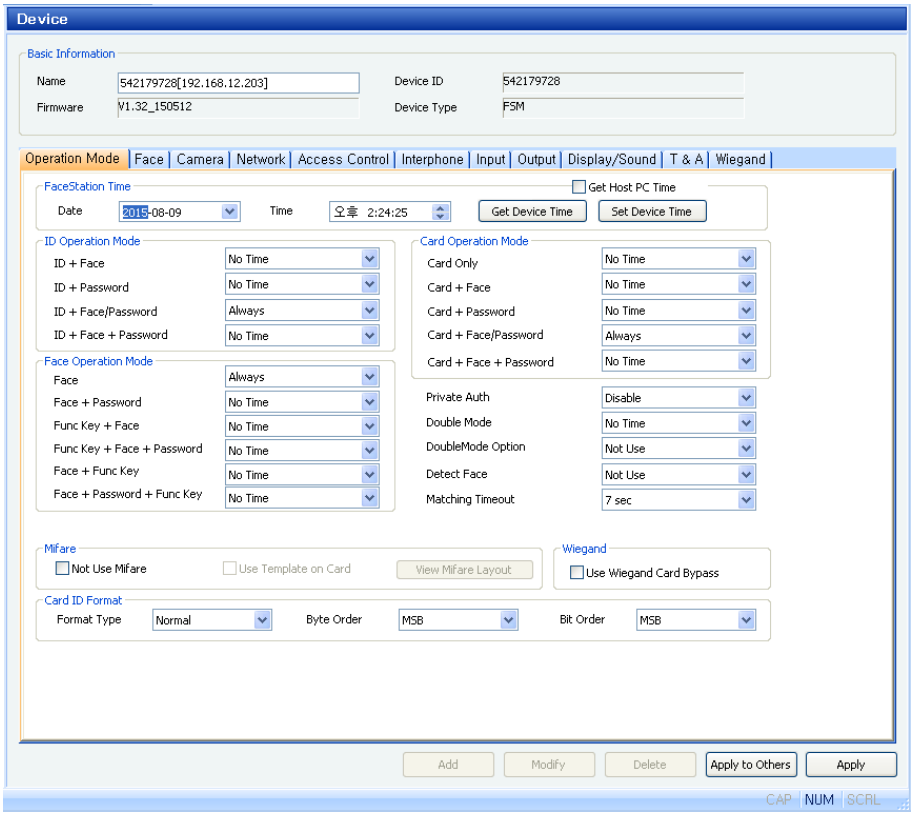
- **Interphone**: Use this tab to set the device to act as an interphone which allows communication between people on either side of the door.
- **Input**: Use this tab to add, modify, or delete input settings for the device.
- **Output**: Use this tab to add, modify, or delete output settings for the device.
- **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
- **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
- **T&A:** Use this tab to configure time and attendance settings.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.

4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.11 Configure a FaceStation Device

To configure a FaceStation device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.8
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
   - **Face** – Use this tab to specify security level and enrollment sensitivity settings for face recognition.
   - **Camera**: Use this tab to assign events, by timezone, that can be performed via the camera and the face detection feature.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
   - **Interphone** : Use this tab to set the device to act as an interphone which allows communication between people on either side of the door.
   - **Input**: Use this tab to add, modify, or delete input settings for the device.
   - **Output**: Use this tab to add, modify, or delete output settings for the device.

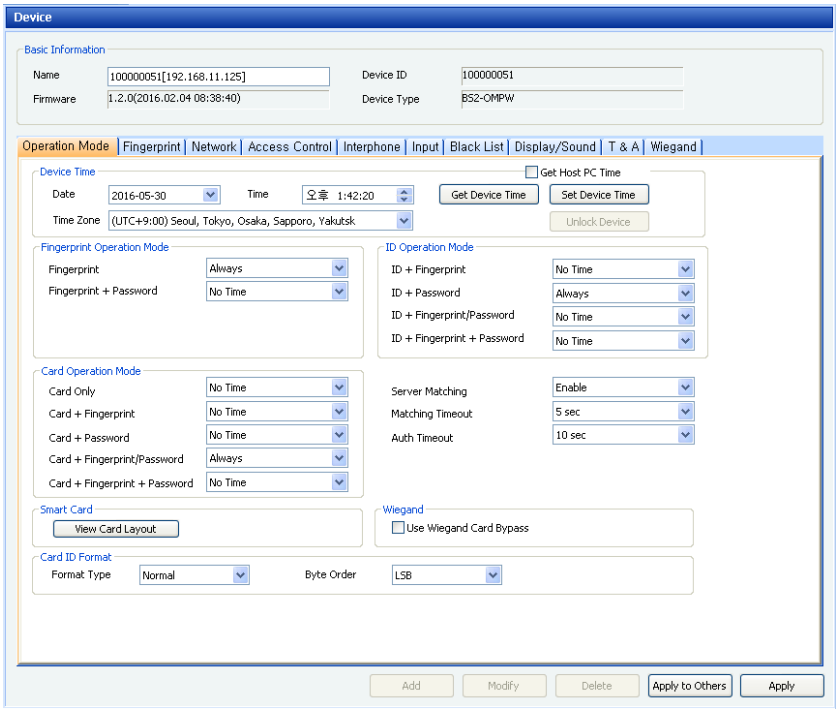
- **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
- **T&A:** Use this tab to configure time and attendance settings.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.163.2.16.

4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.12 Configure a BioStation 2 Device

To configure a BioStation 2 device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.9.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
   - **Fingerprint:** Use this tab to specify security, quality, server matching, and timeout settings for fingerprint recognition.
   - **Network**: Use this tab to specify settings for LAN or serial connections.

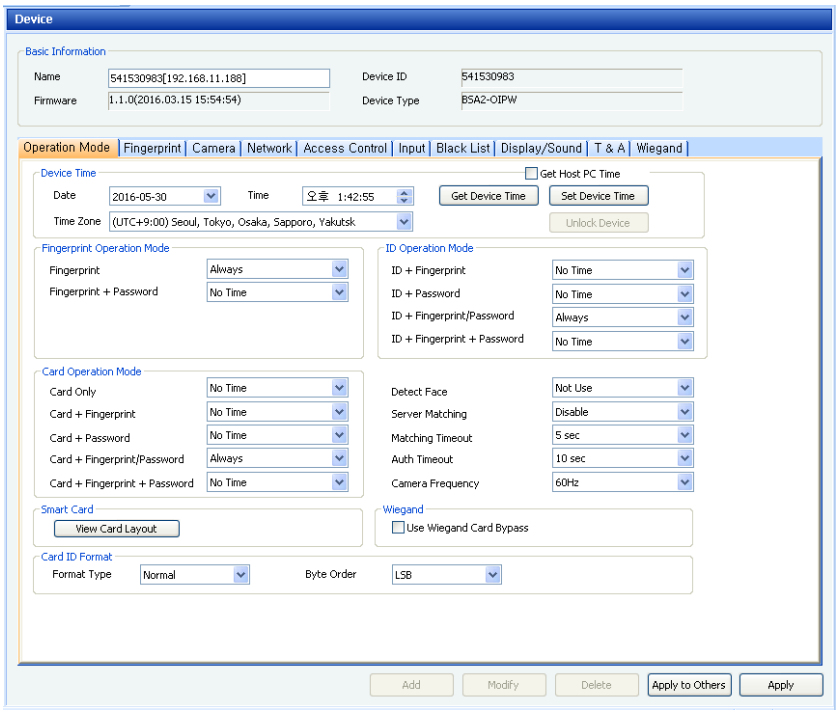
- **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
- **Interphone**: Use this tab to set the device to act as an interphone which allows communication between people on either side of the door.
- **Input**: Use this tab to add, modify, or delete input settings for the device.
- **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
- **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
- **T&A:** Use this tab to configure time and attendance settings.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.

4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.13 Configure a BioStation A2 Device

To configure a BioStation A2 device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



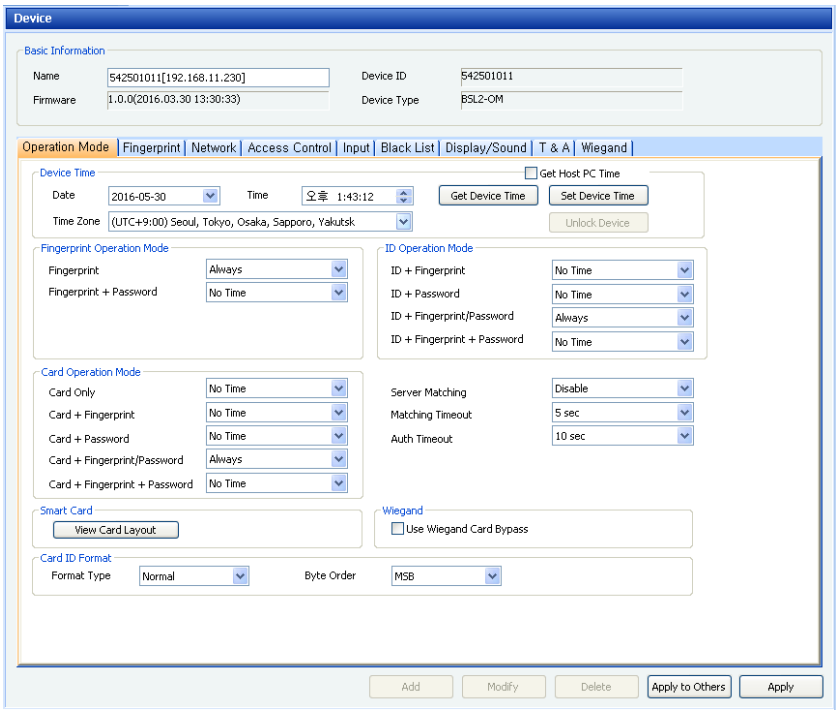
3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.10.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
   - **Fingerprint:** Use this tab to specify security, quality, server matching, and timeout settings for fingerprint recognition.
   - **Camera**: Use this tab to assign events, by timezone, that can be performed via the camera and the face detection feature.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
   - **Interphone**: Use this tab to set the device to act as an interphone which allows communication between people on either side of the door.
   - **Input**: Use this tab to add, modify, or delete input settings for the device.
   - **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
   - **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
   - **T&A:** Use this tab to configure time and attendance settings.
   - **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.
4. When you are finished configuring the device, click **Apply** to save your changes.

5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.14 Configure a BioStation L2 Device

To configure a BioStation L2 device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.11.
   - **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
   - **Fingerprint:** Use this tab to specify security, quality, server matching, and timeout settings for fingerprint recognition.
   - **Network**: Use this tab to specify settings for LAN or serial connections.
   - **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
   - **Interphone**: Use this tab to set the device to act as an interphone which allows communication between people on either side of the door.
   - **Input**: Use this tab to add, modify, or delete input settings for the device.
   - **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature

only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.

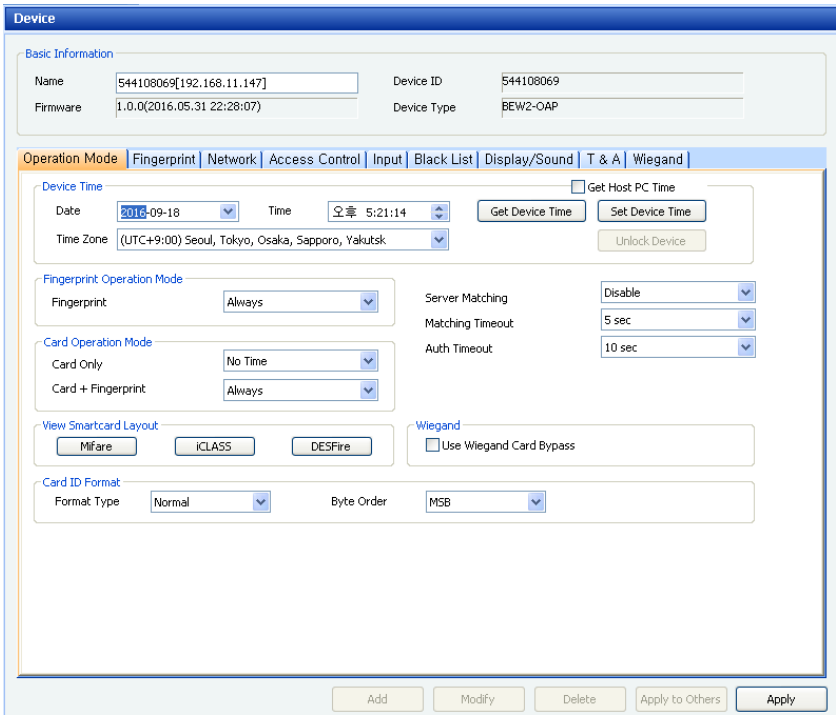
- **Display/Sound**: Use this tab to adjust display or sound settings and add background images and sounds.
- **T&A:** Use this tab to configure time and attendance settings.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.

4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.15 Configure a BioEntry W2 Device

To configure a BioEntry W2 device:

1. Click **Device** in the shortcut pane.
2. Double-click a device name in the navigation pane. This will open a Device pane similar to the one below:



3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.12.

- **Operation Mode**: Use this tab to set the device time or retrieve it from a host PC and adjust settings for operation modes.
- **Fingerprint:** Use this tab to specify security, quality, server matching, and timeout settings for fingerprint recognition.

- **Network**: Use this tab to specify settings for LAN or serial connections.
- **Access Control:** Use this tab to specify entrance limits and default access groups for an individual device.
- **Interphone**: Use this tab to set the device to act as an interphone which allows communication between people on either side of the door.
- **Input**: Use this tab to add, modify, or delete input settings for the device.
- **Black List**: Use this tab to block access through a particular card, e.g. a card which has been stolen or used by a former employee. You can use this feature only when the card mode of the device is set to 'Template on Card'. Adding a user ID or card ID denies access from the users with the matching ID or card.
- **Display/Sound**: Use this tab to configure LED & Buzzer settings according to the event or status.
- **T&A:** Use this tab to configure time and attendance settings.
- **Wiegand**: Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.16.

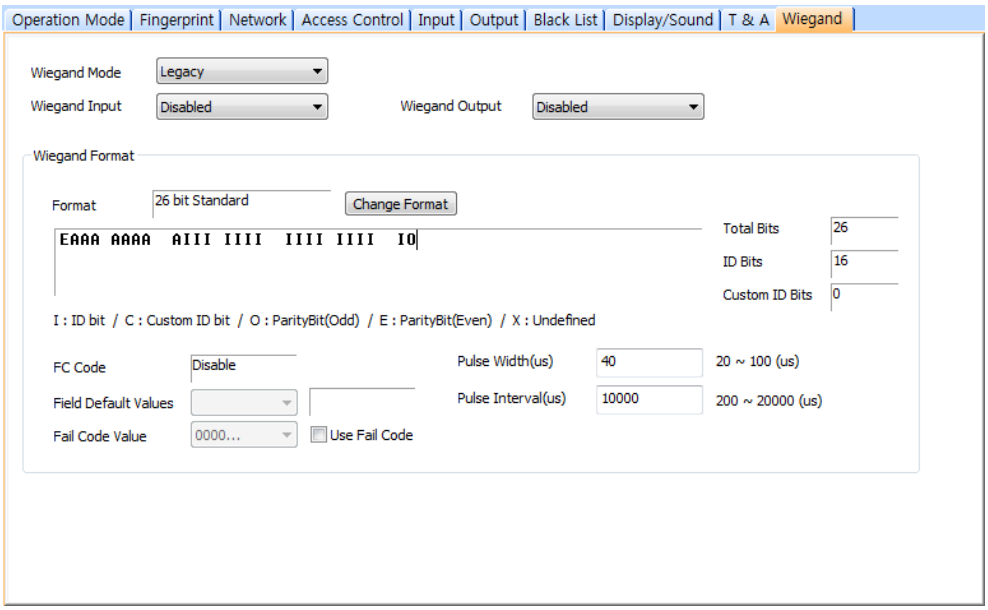
4. When you are finished configuring the device, click **Apply** to save your changes.
5. To apply the same settings to other devices, click **Apply to Others** and select other devices from the **Device Tree** dialog box.

3.2.16 Change Wiegand Formats

From the BioStar interface, you can configure the Wiegand format of a device to control device inputs and outputs.

To configure the Wiegand format:

1. Click **Device** in the shortcut pane.
2. In the navigation pane, click a device name.
3. Click the Wiegand tab in the Device pane.

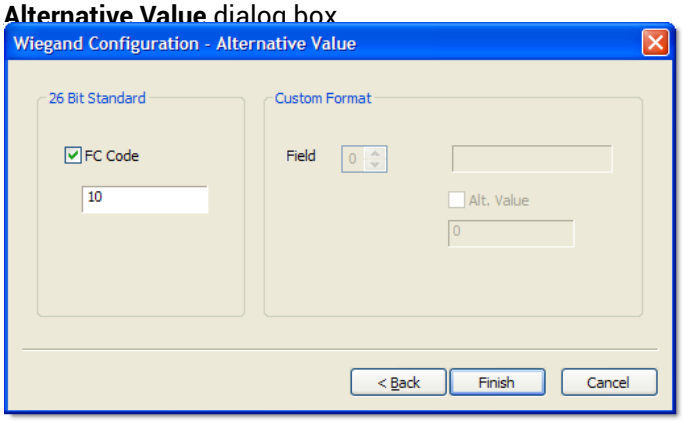


4. Click **Change Format**. This will open the Wiegand Configuration wizard.
5. Click a option button to select one of the following formats:
   - **26-bit Standard**: This format is the most widely used and consists of an 8-bit FC code and a 16-bit ID. You cannot change the bit definition of the format or the parity bits of this format.
   - **Pass-through:** Use this format to customize only the ID bits. During verification, if the ID is recognized, the Wiegand input string will pass through in its original form. You cannot set the parity bits or alternative values of this format. By definition, the pass-through format is useful only when the operation mode is one-to-one (1: 1). In one-to-many (1: N) mode, non-ID bits are set to 0. Pass-through is not supported for BioStation 2, BioStation A2, BioStation L2 and BioEntry W2.
   - **Custom**: With a custom format, you can define the ID bits, parity bits, and alternative values.
6. Use the Wiegand Configuration wizard to customize the Wiegand format to your specifications (see the subsections that follow for more information).
7. When you have completed making changes with the wizard, click **Apply** to save your changes.

3.2.16.1 Configure a 26-bit Wiegand format

When you select a 26-bit format, the only thing you can customize is the FC Code:

1. After selecting the format in the wizard, click **Next** until you reach the **Alternative Value** dialog box.

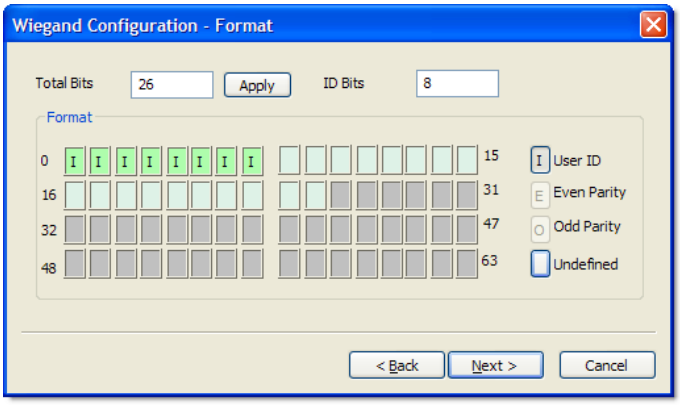


2. Click the FC Code checkbox and enter a new FC Code.
3. Click **Finish** to close the wizard.

3.2.16.2 Configure a pass-through Wiegand format

When you select a pass-through format, you can alter the total number of bits and assign the ID bits:

1. After selecting the format in the wizard, click **Next** to advance to the **Wiegand Configuration - Format** dialog box.



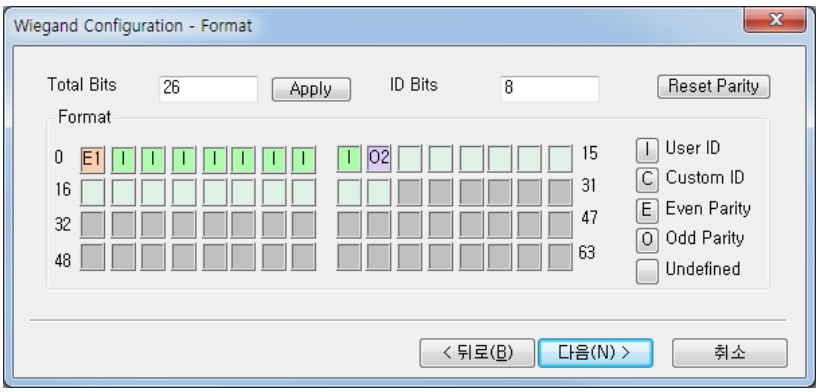
2. If desired, enter a new total number of bits and click **Apply**.
3. Click the User ID button (I) on the right.
4. Assign ID bits by clicking the appropriate squares.
5. Click Next until you reach the **Wiegand Configuration - Alternative Value** dialog box.
6. Click **Finish** to close the wizard.

3.2.16.3 Configure a custom Wiegand format

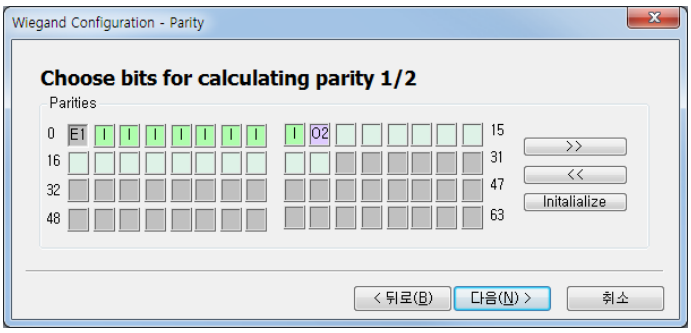
It is able to change entire bit numbers and parity bit numbers, allocate ID bit and custom ID bit section, define parity bit, and set alternative values for specific output data section by selecting user custom Wiegand type.

Configure a custom Wiegand format

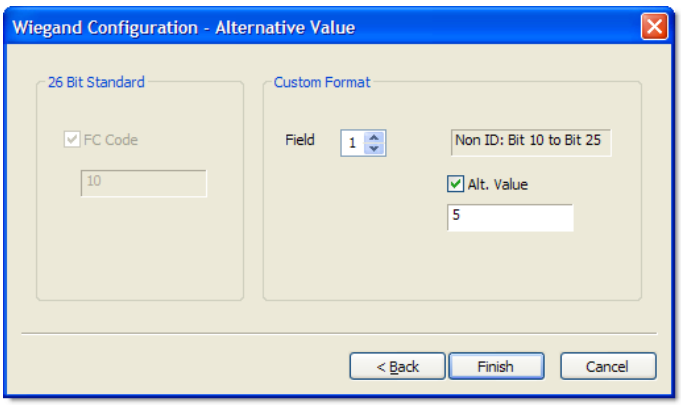
1. After selecting the format in the wizard, click **Next** to advance to the **Wiegand Configuration - Format** dialog box.



2. If desired, enter a new total number of bits and click **Apply**.
3. If parity settings have changed, click the Reset parity button.
4. Click the User ID button (I) on the right and assign ID bits by clicking the appropriate squares.
5. Click the Custom ID button on the right, and then click the square, and set the area for custom ID bit.
6. Click the Even Parity button (E) on the right and assign an even parity bit by clicking on the appropriate squares.
7. Click the Odd Parity button (O) on the right and assign an odd parity bit by clicking on the appropriate squares.
8. Click **Next**.
9. In the **Wiegand Configuration - Parity** dialog box, select the bits that will be used to calculate the first parity bit.



10. As necessary, click **>>** and select the bits that will be used to calculate additional parity bits. You must perform this step for each parity bit you assigned in steps 4 and 5. If necessary, you can click **Initialize** to reset the selection.
11. Click **Next**.
12. In the **Wiegand Configuration - Alternative Value** dialog box, select a field to customize (non-ID bits only).



13. Click the Alt Value checkbox and enter a new value for the output string.
14. Repeat steps 10-11 as necessary to customize the rest of the output string.
15. Click **Finish** to close the wizard.

3.3 Setup Doors

This section describes how to setup doors within the BioStar system. For information about installing physical devices and integrating them with door components, refer to the user guide that accompanies each device.

Attention: A 2.x device (BioStation A2, BioStation 2, BioStation L2, BioEntry W2) cannot configure the door together with a 1.x device (BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation).

3.3.1 Add a Door

To add a door:

1. Click **Doors** in the shortcut pane.
2. In the task pane, click **Add New Door**.
3. Right-click **New Door**, click **Rename**, and type a name for the door.

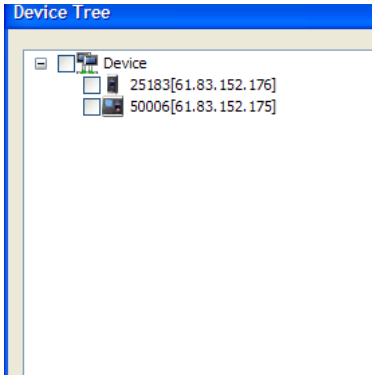
3.3.2 Associate a Device With a Door

BioStar allows you to associate a maximum of two devices with each door. When using two devices on a door, the devices should be connected to each other via RS485. See section 5.2 for an explanation of door settings.

To associate a device with a door:

1. Click **Doors** in the shortcut pane.
2. Right-click a door and click **Add Device**.

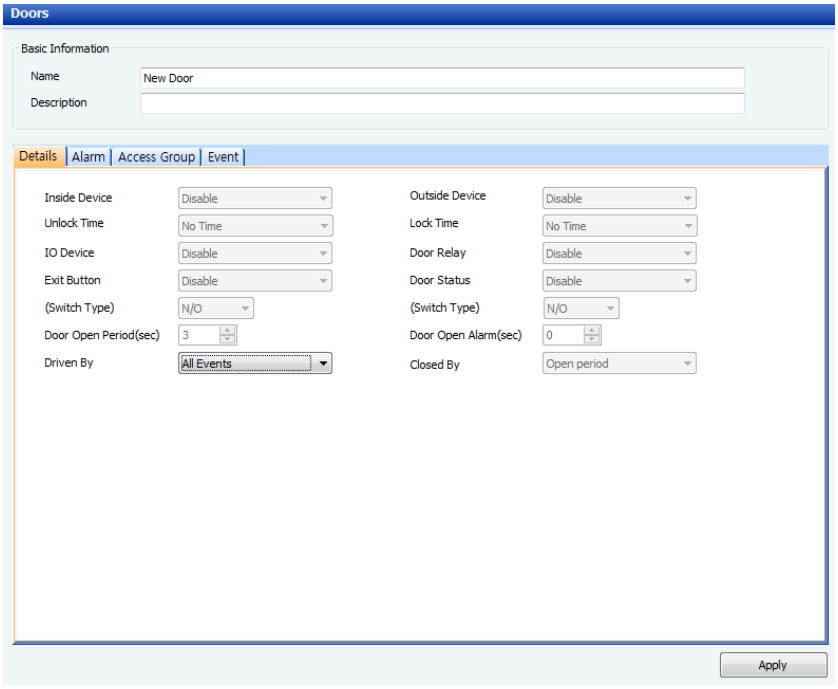
3. Select a device from the **Device Tree** dialog box by clicking the checkbox next to a device name.



4. Click **OK**.

3.3.3 Configure a Door

1. Click **Doors** in the shortcut pane.
2. Click the name of a door in the navigation pane. This will open a Doors pane similar to the one below:



3. Configure door information on the following tabs. For an explanation of door settings, see section 5.2.
   - **Details**: Use this tab to control the interaction between doors, devices, locks, and exit buttons. If you add two devices to a door, you can also use this tab to configure anti-passback settings.

- **Alarm**: Use this tab to specify what actions to take when the door is forced open or held open.
- **Zone**: Use this tab to see the zones associated with a door.
- **Access Control**: Use this tab to see the access groups associated with a door.
- **Event**: Use this tab to retrieve and monitor an event log for the door.

4. When you are finished configuring the device, click **Apply** to save your changes.

3.3.4 Create a Door Group

You can create groups of doors for easier management.

1. Click **Doors** in the shortcut pane.
2. In the navigation pane, right-click *Doors* and click *Add Door Group*.
3. Type a name for the group and press Enter.
4. To add a door to the group, click and drag a door to the group.

3.4 Setup Elevators (Lifts)

This section describes how to setup elevators within the BioStar system. For information about installing physical devices and integrating them with elevator components, refer to the user guide that accompanies each device. BioStar supports up to 120 elevators (lifts).

3.4.1 Add an Elevator

To add an elevator:

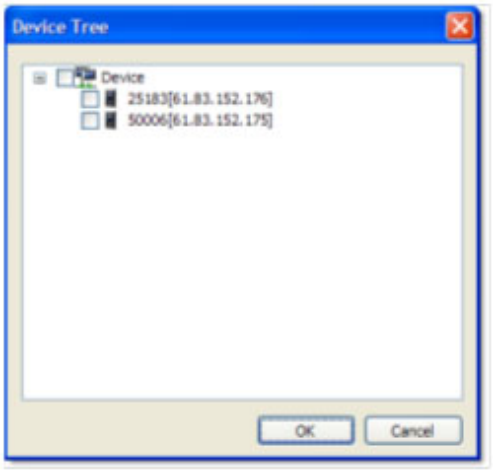
1. Click **Lift** in the shortcut pane.
2. In the task pane, click **Add New Lift**.
3. Right-click **New Lift**, click **Rename**, and type a name for the elevator.

3.4.2 Associate a Device With an Elevator

BioStar allows you to associate Xpass or Xpass S2 devices with a LIFT I/O device to control access to elevators. The LIFT I/O device must be connected to the BioEntry Plus, Xpass or Xpass S2 device via RS485.

To associate an Xpass or Xpass S2 device with an elevator:

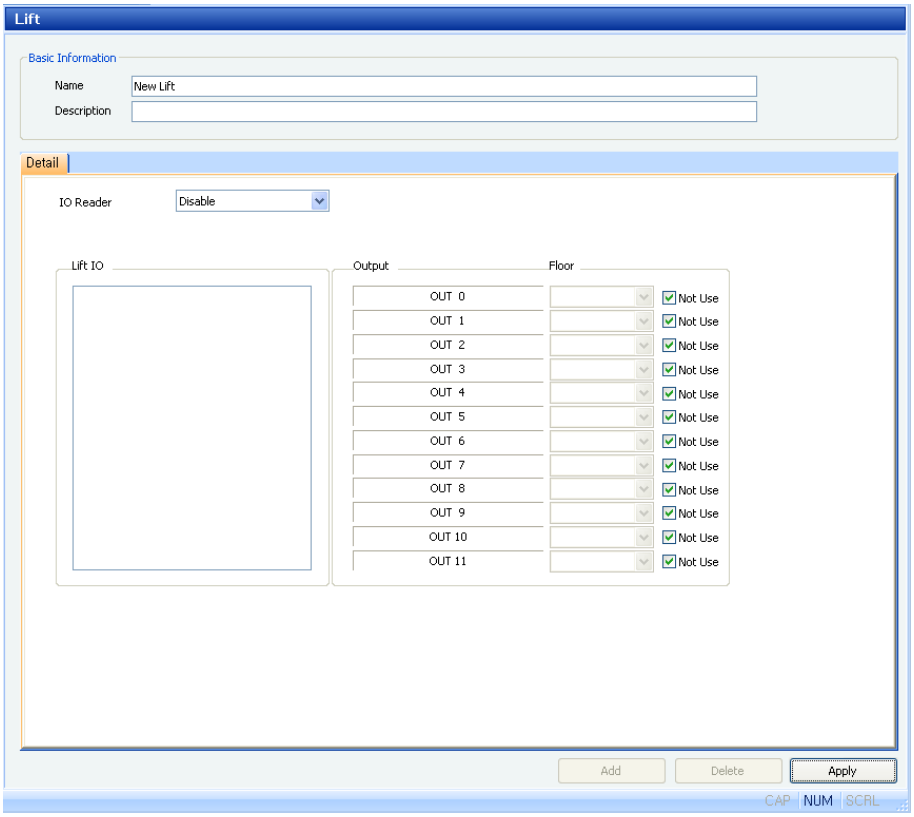
1. Click **Lifts** in the shortcut pane.
2. Right-click an elevator name and click **Add Reader**.
3. Select an Xpass or Xpass S2 device from the **Device Tree** dialog box by clicking the checkbox next to a device name.



4. Click **OK**.

3.4.3 Configure an Elevator

1. Click **Lifts** in the shortcut pane.
2. Click the name of an elevator in the navigation pane. This will open a Lifts pane similar to the one below:



3. Configure elevator information in the following fields:
   - **Lift IO**: Select a LIFT I/O device to view and change settings.
   - **Relay Duration:** Relay Duration is supported in the Detail tab of Lift IO. Default setting range is 10 seconds, and you can set min. 1 second to max. 60 seconds.

Supported by latest regular firmware among Xpass and BioEntry Plus supporting LIFT IO.

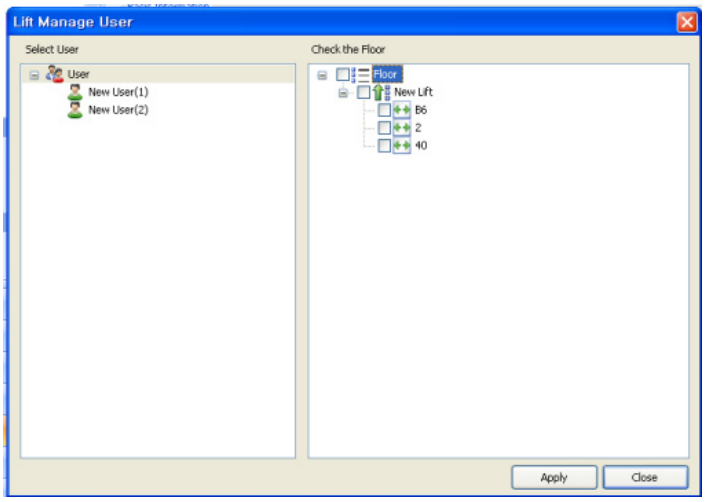
Note: Supported Firmware Versions: BioEntry Plus 1.6, Xpass 1.3

- **Output**: This field lists the avaialble outputs of the LIFT I/O device.
- **Floor**: Use this tab to see the zones associated with a door.
- **Not Use**: Select the checkbox when you do not use the output port of the LIFT I/O device. Clear the checkbox to control aceess to floors by associating outputs with floors.

4. When you are finished configuring the elevator, click **Apply** to save your changes.

3.4.4 Add Users to an Elevator

1. Click **Lifts** in the shortcut pane.
2. Click the name of an elevator in the navigation pane.
3. Click *Lift Manage Users* in the shortcut pane. This will open the **Lift Manage User** dialog box.



4. In the left pane, click a user's name.
5. In the right pane, click the checkboxes next to floors that you wish to assign the user to.
6. Click **Apply** to save your chagnes.

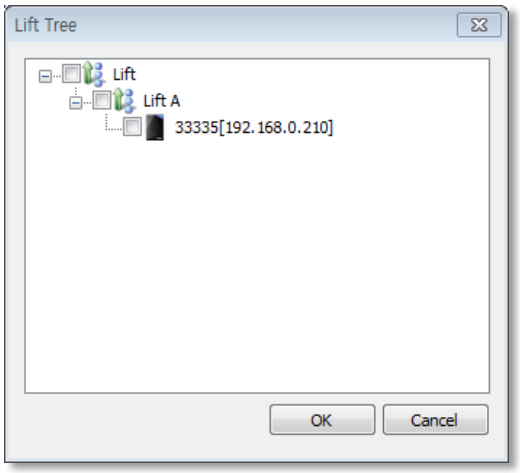
3.4.5 Transfer Settings to an Elevator

Attention: When using BioEntry Plus, Xpass or Xpass S2 devices as lift readers, transferring settings to the device with the User menu will reset all of the settings and user data stored on the device. To preserve the settings, use the *Transfer to Device* function in the Lift menu instead.

To send settings and user data to an Xpass or Xpass S2 device:

1. Click **Lifts** in the shortcut pane.

2. Click **Transfer to Device** in the task pane. This will open the **Lift Tree** dialog box.



3. In the lift tree, select a device or devices by clicking the checkboxes next to device names.
4. Click **Apply** to send the elevator settings to the selected devices.

3.5 Setup Zones

BioStar allows you to provide sophisticated access control with multiple zones. Zones can be used to control the behavior of devices, doors, and other components. In addition, zones can be configured to provide different types of restrictions, such as anti-passback, timed anti-passback, and entrance limits. The sections below describe how to determine which zones to use and how to add and configure zones.

Attention: A 2.x device (BioStation A2, BioStation 2, BioStation L2, BioEntry W2) cannot configure a zone together with a 1.x device (BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation). Also, BioStation A2, BioStation 2, BioStation L2 and BioEntry W2 can configure only an anti-passback zone and a fire alarm zone.

3.5.1 Determine Which Zones to Use

In total, the BioStar system supports seven types of zones:

- **Access zone**: Use this zone to synchronize user or log information. If you select the user synchronization option, user data enrolled at the devices will be automatically propagated to other connected devices. If you select the log synchronization option, all log records will be written to the master device (in addition to the server), so that you can check log records of member devices. For information about customizing access zones, see section 5.3.5.

- **Anti-passback zone**: Use this zone to prevent a user from passing his or her card back to another person or using his or her fingerprint to allow someone else to gain entry. The zone supports two types of anti-passback restrictions: soft and hard. When a user violates the anti-passback protocol, the soft restriction will record the action in the user's log. The hard restriction will deny access and record the event in the log when the anti-passback protocol is violated. For information about customizing anti-passback zones, see section 5.3.1.
- **Entrance limit zone**: Use this zone to restrict the number of times a user can enter an area. The entrance limit can be tied to a timezone, so that a user is restricted to a maximum number of entries during a specified time span. You can also set time limits for reentry to enforce a timed anti-passback restriction. For information about customizing entrance limit zones, see section 5.3.2.
- **Alarm zone**: Use this zone to group inputs from multiple devices into a single alarm zone. Devices in the alarm zone can be simultaneously armed or disarmed via an arm or disarm card or a key. For more information about configuring alarm zones, see sections 3.5.2.4, 3.5.2.5, 3.5.2.6 and 5.3.3.
- **Fire alarm zone**: Use this zone to control how doors will respond during a fire. External inputs can be fed into the BioStar system to automatically trigger door releases or perform other actions. For more information about customizing fire alarm zones, see section 5.3.4.
- **Muster zone**: Use this zone to monitor and track employees during an emergency or to perform a “roll call” where employees are required to be present in a particular area at a particular time. Muster zone allows administrators to determine if any employee has not reported to the muster area and, if any employee is unaccounted for, take the necessary actions to locate them. For more information about customizing muster zone, see section 5.3.6.
- **Interlock zone**: Use this zone to create an interlock area with two doors equipped with devices. When an external input indicates that one door is open, the other door is automatically locked to provide a secure interlock area. A reader-equipped door that does not belong to any other zone can be used to create up to four interlock zones (four zones maximum per reader). For more information about configuring an interlock zone, see section 5.3.7.

3.5.2 Add and Configure Zones

When you add a zone, you can use the four tabs in the Zone pane to configure the zone. For an explanation of zone settings, see section 5.3.

- **Details:** Add devices and specify inputs or other parameters for a zone.
- **Alarm**: Specify alarm actions and outputs.
- **Access Group**: Apply access groups to a zone (not available for fire alarm zones).
- **Event**: View events associated with a zone.

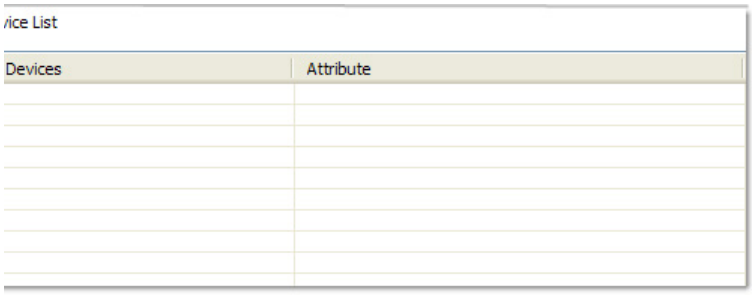
3.5.2.1 Add a zone

To add a new zone:

1. Click **Doors** in the shortcut pane.
2. In the navigation pane, right-click *Zone*.
3. Click *Add Zone*.
4. Type a name for the zone in the Name field.
5. Select a zone type from the drop-down list (see section 3.5.1 for zone descriptions).
6. Press **OK**. The Zone pane will appear on the right side of the screen.

3.5.2.2 Add a device to a zone

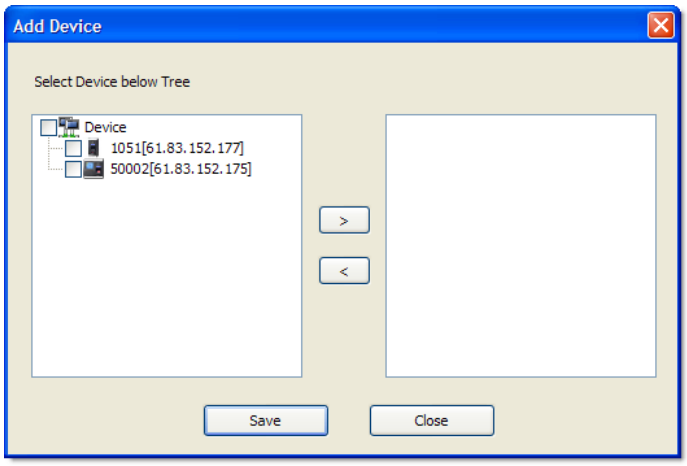
To implement the protocols of a zone, you must associate devices with the zone. The Details tab (in the Zone pane) contains a Device List that shows each device associated with a zone (see below).



Attention: BioStation A2, BioStation 2, BioStation L2 and BioEntry W2 can configure only an anti-passback zone and a fire alarm zone.

To add a device to a zone:

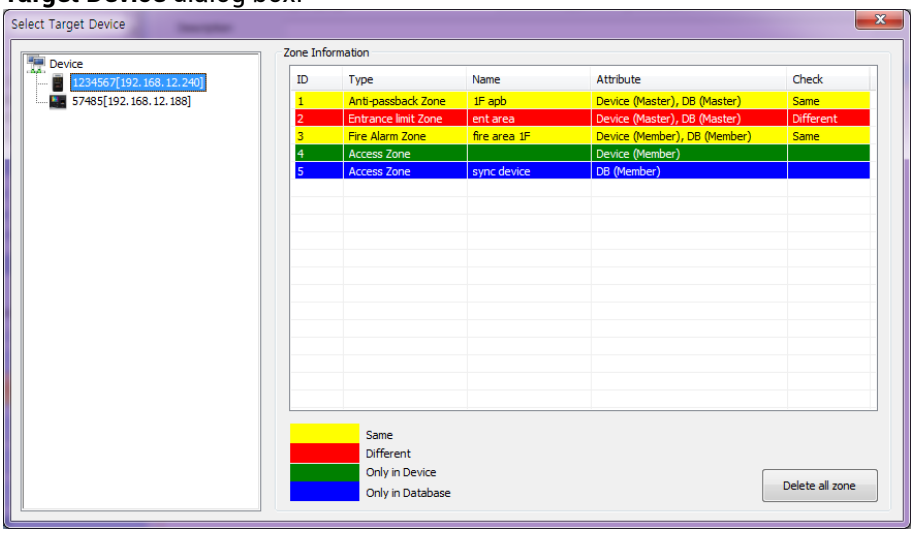
1. Click **Doors** in the shortcut pane.
2. In the navigation pane, click the name of a zone.
3. In the Zone tab, at the bottom of the Device List, click **Add Device**. This will open the **Add Device** dialog box.



4. Select a device (or multiple devices) from the list and click **>**.
   - **Anti-passback zones**: When the Select Zone Attribute pop-up appears, select an attribute from the drop-down list (*In Device* or *Out Device*).
   - **Alarm zones**: When the Select Zone Attribute/Type pop-up appears, select a device attribute from the drop-down list (*General*, *Arm*, *Disarm*, or *Arm/Disarm*). If you select an arm or disarm attribute (or *Arm/Disarm*), click the *Card* or *Key* option button to specify how to arm or disarm zones, and then press **OK**. For more information about arming or disarming zones, see section 3.5.2.5.
5. Press **Save** to add the devices to the list.

To check zones configured in each device:

1. Click **Doors** in the shortcut pane.
2. In the task pane, click **Manage Zone in Device**. This will open the **Select Target Device** dialog box.



3. Click a device name in the list on the left to display zone information contained in the device.

- Yellow: Indicates that the configuration data in both the device and the server are identical.
- Red: Indicates that the configuration data in the device and the server are different.
- Green: Indicates that the configuration data are stored to the device only.
- Blue: Indicates that the configuration data are stored to the server only.

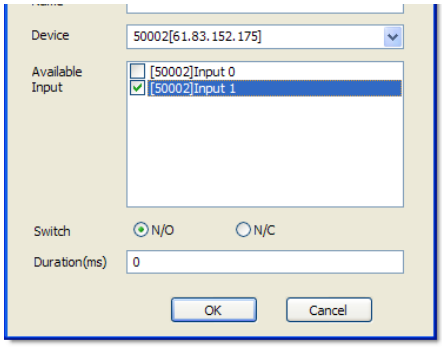
4. Optional: To delete all zones from the device, select a device and click **Delete all zone** in the lower-right corner of the screen.

3.5.2.3 Configure zone inputs

When adding devices to an alarm or fire alarm zone, you must also configure the zone inputs.

To configure inputs:

1. Click **Doors** in the shortcut pane.
2. In the navigation pane, click the name of a zone.
3. In the Zone tab, at the bottom of the Device List, click **Add Input**. This will open the **Add Zone Input** dialog box.



4. Type a name for the input in the Name field.
5. Select a device from the drop-down list.
6. Select one of the available inputs by clicking the checkbox next to the appropriate input.
7. Select the normal position of the input (*N/O-normally open* or *N/C-normally closed*).
8. Set the duration (in milliseconds) of the input signal.
9. Click **OK** to add the input to the Input List.

3.5.2.4 Configure alarm actions and outputs

Configure alarm actions to specify what alerts to receive, if any, and which ports and relays to use for alarm outputs. The Alarm tab (in the Zone pane) offers the

following options for all zones except access zones. For more information about alarms, see sections 3.5.2.5 and 3.10.

- **Program Sound**: Set a sound to be emitted by the software (at the host computer or BioStar Server). To add custom sounds, please see section 3.10.1.2.
- **Device Sound**: Set a sound to be emitted by a particular device.
- **Send Email**: Create an email alert to send when an alarm is activated and select recipients or email alerts. For more information about email alerts, see section 3.10.2.
- **Output Device**: Specify a device that will send an alarm signal to an external device, such as an alarm siren.
- **Output Port**: Specify the port to use for an output signal.
- **Output Signal**: Specify a type of output signal.

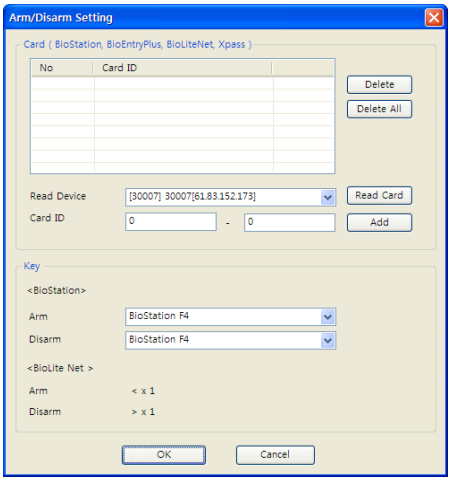
3.5.2.5 Configure arm and disarm settings

After adding an alarm zone, you can configure the actions that will arm and disarm the zone.

Attention: BioStation A2, BioStation 2, BioStation L2 and BioEntry W2 can configure only an anti-passback zone and a fire alarm zone.

To configure arm and disarm settings:

1. Click **Doors** in the shortcut pane.
2. In the navigation pane, click the name of an alarm zone.
3. Click the Details tab in the Zone pane.
4. Click **Setup** to the right of Arm/Disarm Type. This will open the **Arm/Disarm Setting** dialog box.



5. To configure cards for arming or disarming zones:

a. Select a device from the Read Device drop-down list.
b. Click **Read Card**. The LED on the device you selected will begin to flash.
c. Place the card on the device.
d. When the card has been read, click **Add**. The card can now be used to arm or disarm devices in the alarm zone.

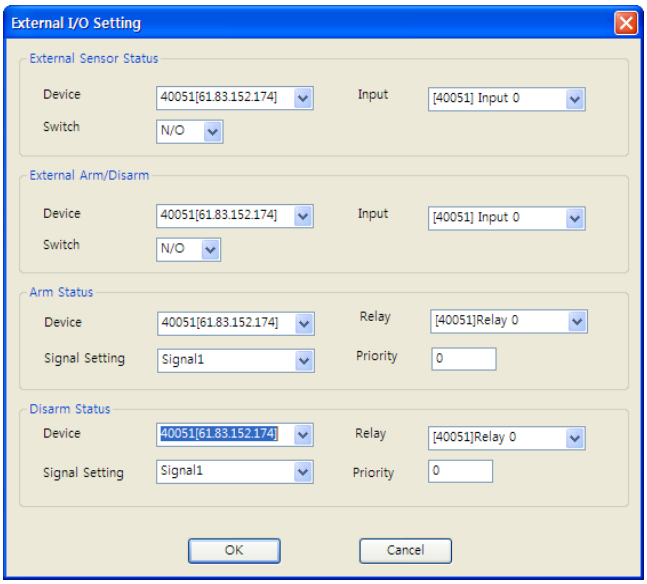
6. To configure device keys for arming or disarming zones (BioStation devices only):
   a. Select a key that will arm devices from the first drop-down list.
   b. Select a key that will disarm devices from the second drop-down list.
7. When you are finished configuring the arm and disarm settings, click **OK**.

3.5.2.6 Configure external input/output settings

Instead of manually arming or disarming alarm zones, you can configure the BioStar system to automatically determine when to arm or disarm alarm zones based on the status of a specified input. You can also prevent the BioStar system from arming an alarm zone when a monitored input is in a not-ready position. Finally, you can configure the system to send a specified signal to an external output when it arms or disarms alarm zones. External input/output settings are available in BioStation V1.8, BioEntry Plus V1.4, BioEntry W V1.0, BioLite Net V1.2, Xpass and Xpass S2 V1.0, X-Station V1.0, BioStation T2 and FaceStation V1.0 or higher.

To configure external input/output settings:

1. Click **Doors** in the shortcut pane.
2. In the navigation pane, click the name of an alarm zone.
3. Click the Details tab in the Zone pane.
4. Click **Setup** to the right of External Input/Out. This will open the **External I/O Setting** dialog box.



5. Configure the following input/output settings as desired:
   - To prevent the BioStar system from arming an alarm zone:
   a. Under External Sensor Status, select a device from the Device drop-down list.
   b. Select an input from the Input drop-down list.
   c. Select the position of the input (*N/O – normally open* or *N/C – normally closed*) that will prevent the system from arming the alarm zone.
   - To allow the BioStar system to automatically arm or disarm an alarm zone:
   a. Under External Arm/Disarm, select a device from the Device drop-down list.
   b. Select an input from the Input drop-down list.
   c. Select the position of the input (*N/O – normally open* or *N/C – normally closed*) that will allow the system to arm the alarm zone. The other position will allow the system to disarm the alarm zone.
   - To send an arm signal to an external device, such as an alarm signal:
   a. Under Arm Status, select a device from the Device drop-down list.
   b. Select a relay from the Relay drop-down list.
   c. Select a type of signal from the Signal drop-down list.
   d. Specify a priority level in the Priority field.
   - To send a disarm signal to an external device, such as an alarm signal:
   a. Under Disarm Status, select a device from the Device drop-down list.
   b. Select a relay from the Relay drop-down list.
   c. Select a type of signal from the Signal drop-down list.
   d. Specify a priority level in the Priority field.
6. When you are finished configuring the external input/output settings, click **OK**.

3.5.2.7 Select access groups

The Access Group tab (in the Zone pane) allows you to specify access groups that can bypass the normal restrictions set for the zone. For example, you may choose a particular access group to be exempt from the restrictions of an anti-passback zone. For alarm zones, this tab allows you to specify access groups that can arm and disarm alarms. To select an access group, please click the checkbox next to a group name and then click **Apply**.

3.5.2.8 View zone events

The Event tab (in the Zone pane) provides a listing of log events for a particular zone. You can set a date range with the drop-down calendars and view a report of events by clicking **Get Log**. For more information about monitoring and viewing event logs, see section 4.1.

3.6 Setup Users

You will need to use a fingerprint scanner to capture each user's fingerprints. For this reason, it may be helpful to have a terminal connected to the system at a registration center, such as a human resources or security office. BioStation, BioEntry Plus, BioEntry W, or BioLite Net devices can be used for fingerprint scanning when networked to the BioStar server, or the BioMini USB device can be connected directly to a BioStar client to provide convenient fingerprint scanning at a registration location.

When adding users, you will first need to create a user account. Once the account has been created, you can register fingerprints and access cards or edit user details as desired.

3.6.1 Create a User Account

User data is controlled via a user account. You can create new accounts for users or retrieve user data from a device. To retrieve user data from a device, please see section 3.6.5.3. To migrate user data from an existing BioAdmin database, see section 2.7.

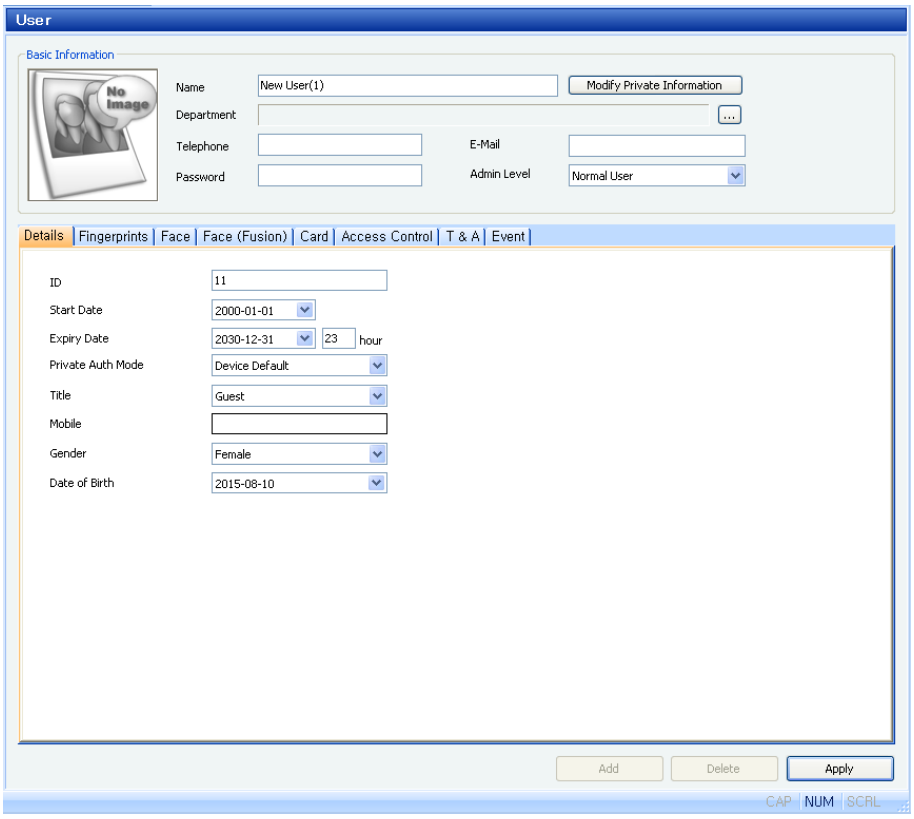
To create a new department:

1. Click **User** in the shortcut pane.
2. In the navigation pane, right-click *User* that is top level of department and then click **Add Department**.
3. Enter a name for the department.

Note: Up to four department levels can be created.

To create new user accounts:

1. Click **User** in the shortcut pane.
2. In the navigation pane, right-click *User* or a department name and click *Add User*. This will open a User pane similar to the one below.



3. Add details of the user's account in the User pane:

- **Name**: Enter the user's name.
- **Department**: Enter a department or click the ellipsis button (...) to select from departments you have added to the BioStar system.
- **Telephone**: Enter the user's telephone number (digits only—no characters are allowed in this field).
- **E-mail**: Enter the user's email address.
- **Password**: Enter the user's password, if desired.
  Note: Passwords saved in FaceStation devices are not compatible with other devices. When transferring data from a FaceStation device to another type of device, you must create new passwords for the other device.
- **Admin Level**: Select the user's BioStar administration level (*Normal User* or *Admin User*).
- **ID**: Enter an identification number for the user.
- **Start Date**: Set a beginning date that the user can obtain authorization via the BioStar system.
- **Expiry Date**: Set a date that the user's account will expire (you can also specify the hour that the account will expire).
- **Title**: Select a title for the user (*Guest*, *President*, *Director*, *General Manager*, *Chief*, *Assistant Manager*, or custom title).
- **Mobile**: Enter a mobile telephone number for the user.
- **Gender**: Select the user's gender.

- **Date of Birth**: Select the user's date of birth from the drop-down calendar.

Note: You can add a photo of the user or a private message by clicking Modify Private Information.

4. Register fingerprints (see section 3.6.2), face images (see section 3.6.3), and access cards (see section 3.6.4) as necessary.
5. When you are finished adding details to the user's account, click **Apply**.

3.6.2 Register Fingerprints

BioStar provides an option for encrypting fingerprint templates. If you choose to use this option, you should set the encryption before capturing fingerprint scans. Any previously-captured fingerprint templates will be rendered unusable when you activate the encryption. For more information about encrypting fingerprints, see section 4.7.

When registering fingerprints, it is important to capture quality images. Before registering fingerprints, ensure that the candidate's fingers are clean and dry. You may need to ask the candidate to clean his or her fingers just prior to registration. If a candidate has excessively dry skin, ask him or her to moisten the fingertips slightly by breathing warm air on them just prior to registration.

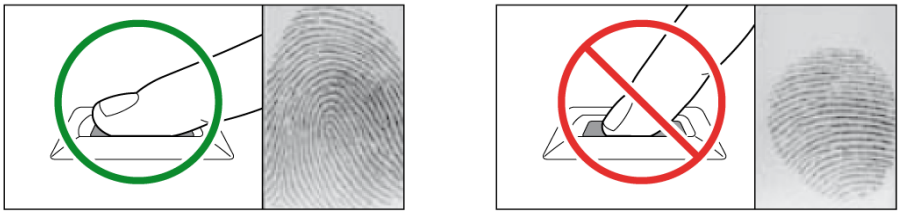
When registering fingerprints, keep the following tips in mind:

- You must register the same finger twice (two templates). You can register a total of two fingers (a total of four templates) per user.
- Fingers with scars, worn fingerprints, or other physical damage may be poor choices for registration.
- It may be necessary to delete and recapture an image of a fingerprint if the candidate experiences low acceptance rates.

3.6.2.1 Place fingers on the sensor

To ensure good quality fingerprints, candidates must place as much of the finger pad (the soft part opposite the fingernail) on the sensor as possible. Suprema recommends using index or middle fingers, because they are typically easier for users to correctly place on the sensor. To properly place a finger on the sensor, candidates should lay the finger flat, so that the pad side covers most of the sensor and the finger is nearly perpendicular to the sensor.

The image below illustrates both correct and incorrect placement of a finger on the sensor.



Attention: A fingerprint cannot be registered with a 2.x device connected as a slave device.

3.6.2.2 Register fingerprints

BioStar allows you to register up to ten fingerprints per user. However, some devices can only store a limited number of fingerprints:

Device	Number of Fingerprints
BioEntry Plus	**2**
BioEntry W	
BioLite Net	
BioStation	**5**
BioStation T2	**10**
BioStation A2	
BioStation 2	
BioStation L2	
BioEntry W2	

When fingerprints are distributed from BioStar, the device will receive the maximum number of fingerprints, beginning with the first stored fingerprint scan.

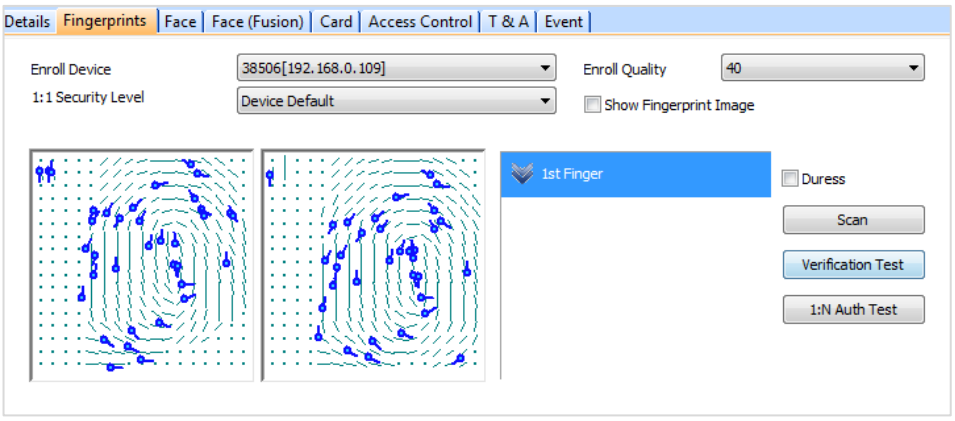
If desired, one of the fingerprints can be used as a duress signal that will trigger alarms when a candidate is forced to access an area. When registering duress fingerprints, keep the following tips in mind:

- A duress finger cannot be used for normal access
- The duress finger should appear to be a natural choice (i.e., the little finger is an unusual choice and may indicate to a perpetrator that the candidate is triggering an alarm)

- Candidates should be educated about what occurs when the duress finger is used (e.g., the duress finger may trigger automatic door locks or silent alarms).

To register fingerprints:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. Click the Fingerprints tab in the User pane.



4. Select the device you will use for scanning fingerprints from the **Enroll Device** drop-down list.
5. Select a security level from the **1:1 Security Level** drop-down list.
6. Specify any of the following options, as desifred:
   - **Enroll Quality**: Set the quality of fingerprints to be enrolled to increase authentification efficiency. The quality of a fingerprint is determined by multiple factors incluing data on its minutiae distribution. You can specify four values (20, 40, 60, 80) and selecting the higher numbers will improve the quality of a fingerprint but can reduce the chances of a fingerprint being enrolled. Please note that this option is only avaiable on BioStar Standard Edition.
   - **Show Fingerprint Image**: Specify whether to display a fingerprint image on the screen. Fingerprint images are not saved in the database of BioStar server and you can only save individual images on your PC if necessary.
7. Click **Add** at the bottom right of the User pane to create an empty slot for registering a fingerprint.
8. In an empty finger slot, press **Scan** and then have the user place his or her finger on the scanner twice, as prompted by the BioStar interface.
9. If desired, click the checkbox next to the Duress option to set this fingerprint as the duress signal.
10. Repeat steps 6-8 to register the rest of fingerprints.
11. Click **Apply** to save your changes.

12. Validate the submitted fingerprints by clicking either one or both of the following two options:
    - **Verification Test**: Compare a newly-scanned fingerprint to only the stored fingerprint templated collected from a prior enrollment.
    - **1: N Auth Test**: Match a newly-scanned fingerprint against multiple fingerprint templates stored in the server.

3.6.2.3 Enroll users via command cards

After issuing command cards, you can enroll users directly from a BioEntry Plus, BioEntry W, or Xpass device. For more information about issuing command cards, please see section 3.2.6.1 and 3.2.8.1.

To enroll a user on a BioEntry Plus or BioEntry W device via a command card:

1. Place an enroll card (command card) on a BioEntry Plus or BioEntry W device.
2. If authorization is required, an administrator must scan his or her fingerprint to continue.
3. To capture only fingerprints, have the user place his or her finger on the scanner two times (as prompted by the device).
4. To capture fingerprints and issue an access card, place the card on the device first. Then, have the user place his or her finger on the scanner two times (as prompted by the device).

To enroll a user on an Xpass device via a command card:

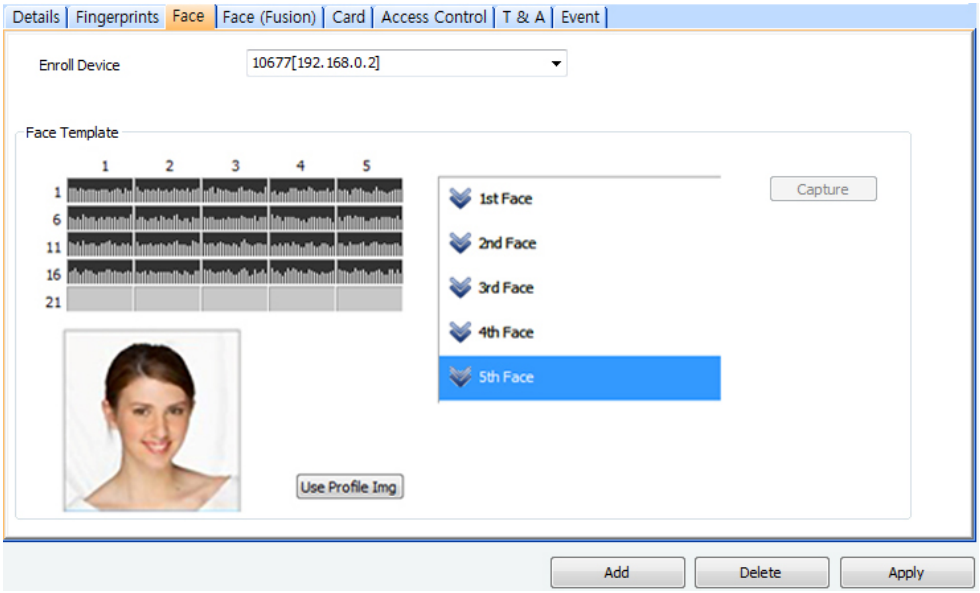
1. Place an enroll card (command card) on an Xpass device.
2. If authorization is required, an administrator must place his or her access card on the device to continue.
3. Place the user's access card on the device.
4. Place the enroll card again on the device to confirm the action.

3.6.3 Capture Face Images

With camera-equipped devices, such as FaceStation, you can capture images of users' faces and use those images for authentication via BioStar's face detection technology. BioStar matches a still image of the user's face during authentication with captured face images in the BioStar server database. Face detection can be used simultaneously with fingerprint recognition for highly secure biometric access control. For more information about face detection settings, please see section 5.4.3.

To capture face images with FaceSation devices:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. Click the Face tab in the User pane.



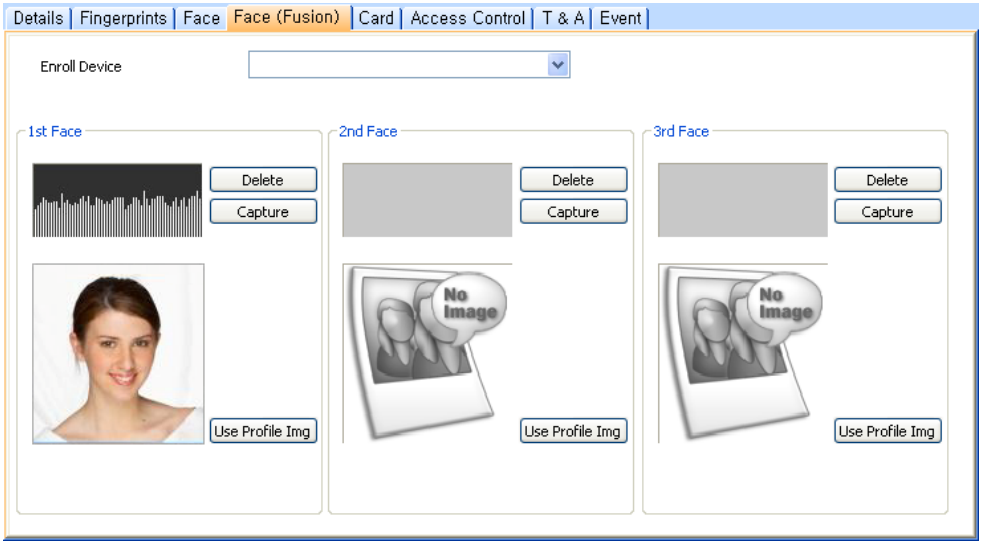
4. Select the *Enrollment Device* you will use for capturing face images from the drop-down list.
5. Click **Add** at the bottom right of the screen to add face(from the 1st Face to the 5th Face).

Note: FaceStation supports up to 5 different user faces to ensure the most accurate face detection at all times, regardless of the different hair styles, make-ups or eye glasses the user might wear.

6. Click the newly added face, click Capture, then follow the instructions prompted by the enrollment device. Repeat steps 5~6 to add more faces.
7. Click Use Profile Img to use the currently registered and selected face image as the user's profile image in the **User** pane.
8. Click **Apply** to save your changes.

To capture face images with devices:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. Click the Face (Fusion) tab in the User pane.



4. Select the enrollment device you will use for capturing face images from the drop-down list.
5. In the 1st Face section, click **Capture**, and then have the user align his or her face with the camera, as prompted by the device.
6. If desired, click **Use Profile Img** to use the image assigned to the user's profile instead of capturing a new image.
7. Repeat steps 5-7 in the 2nd Face and 3rd Face sections to capture additional face images.
8. Click **Apply** to save your changes.

3.6.4 Issue Access Cards

Suprema manufactures access control devices that support multiple types of access cards, as listed below:

- EM4100: BioStation, BioEntry Plus, and BioLite Net, BioStation 2, BioStation L2, BioEntry W2
- MIFARE®: BioStation, BioEntry Plus, BioEntry W, BioLite Net, BioStation 2, BioStation L2, BioEntry W2
- iCLASS®: BioEntry Plus, BioStation 2, BioStation A2, BioEntry W2
- FeliCa®: BioEntry Plus, BioStation 2, BioStation A2, BioStation L2, BioEntry W2
- HID prox: BioStation, BioEntry Plus, BioStation 2, BioStation L2, BioEntry W2

EM4100 and HID cards require only a card ID to complete card registration, while MIFARE and iCLASS cards support two operation modes: Card Serial Number (CSN) and Template-on-Card modes. FeliCa cards support only the CSN mode. When using the CSN mode, you can read the serial number just as you would for an EM4100 or HID card. When using Template-on-Card mode, you must record the user information, including fingerprint templates, directly to the card.

Follow the procedures below to issue the appropriate type of card and then add it to the user's account.

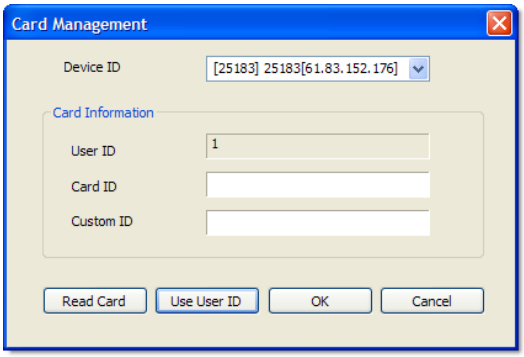
Note: Only one card can be issued and used for BioStation 2, BioStation A2, BioStation L2 or BioEntry W2.

Attention: A card cannot be issued with a 2.x device connected as a slave device.

3.6.4.1 Issue EM4100 cards

To register a EM4100 card for a user:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. In the User pane, click the Card tab.
4. Select a "EM4100" from the Card Type drop-down list.
5. Click **Card Management**. This will open the **Card Management** dialog box.



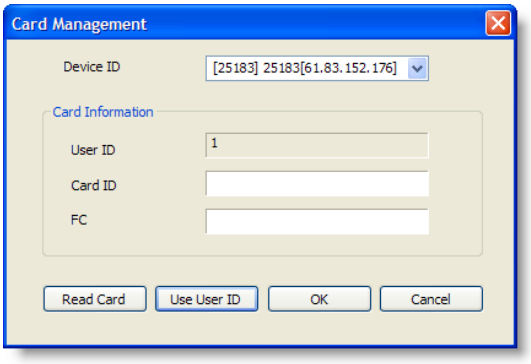
6. Select a Device ID from the drop-down list.
7. Enter a card ID (32 bits) and custom ID (8 bits) either manually or by reading from the card (you can also click **Use User ID** to insert the user's ID in these fields):
   - To enter the data manually, type the card ID and custom ID in the corresponding fields, click **OK**, and then skip to step 8.
   - To read the data from the card, click **Read Card** (the LED on the device you selected will begin flashing) and then place the card on the device. After the card has been read, click **OK**.

8. Click **Apply** to save the card to the user's account.

3.6.4.2 Issue HID proximity cards

To register a HID proximity card for a user:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. In the User pane, click the Card tab.
4. Select "HID Prox" from the Card Type drop-down list.
5. Click **Card Management**. This will open the **Card Management** dialog box.

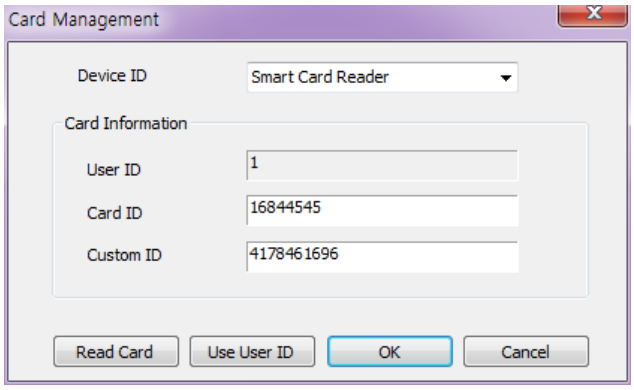


6. Select a Device ID from the drop-down list.
7. Enter a card ID and facility code (FC) either manually or by reading from the card (you can also click **Use User ID** to insert the user's ID in these fields):
   - To enter the data manually, type the ID and facility code in the corresponding fields, click OK, and then skip to step 8.
   - To read the data from the card, click Read Card (the LED on the device you selected will begin flashing) and then place the card on the device. After the card has been read, click OK.
8. Click **Apply** to save the card to the user's account.

3.6.4.3 Issue FeliCa cards

To register a FeliCa card for a user:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. In the User pane, click the Card tab.
4. Select "FeliCa" from the Card Type drop-down list.
5. Click **Card Management**. This will open the **Card Management** dialog box.



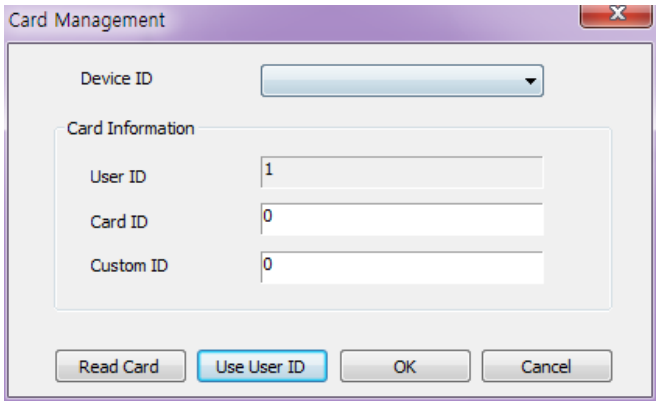
6. Select a device or Smart Card Reader from the **Device ID** drop-down list.
7. Enter a card ID and custom ID either manually or by reading from the card (you can also click **Use User ID** to insert the user's ID in these fields):
   - To enter the data manually, type the card ID and custom ID in the corresponding fields, click OK, and then skip to step 8.
   - To read the data from the card, click Read Card (the LED on the device you selected will begin flashing) and then place the card on the device. After the card has been read, click OK.
8. Click **Apply** to save the card to the user's account.

3.6.4.4 Issue MIFARE, DESFire or iCLASS CSN cards

MIFARE, DESFire and iCLASS CSN cards work much like EM4100 and HID cards, in that they store an uneditable card serial number (CSN) for a user.

To register a card for a user:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. In the User pane, click the Card tab.
4. Select "Mifare CSN" or "iCLASS CSN" from the Card Type drop-down list.
5. Click **Card Management**. This will open the **Card Management** dialog box.



6. Select a Device ID or Smart Card Reader from the drop-down list.

7. Enter a card ID either manually or by reading from the card (you can also click **Use User ID** to insert the user's ID in these fields):
   - To enter the data manually, type the ID and facility code in the corresponding fields, click OK, and then skip to step 8.
   - To read the data from the card, click Read Card (the LED on the device you selected will begin flashing) and then place the card on the device. After the card has been read, click OK.
8. Click **Apply** to issue the card to the user's account.

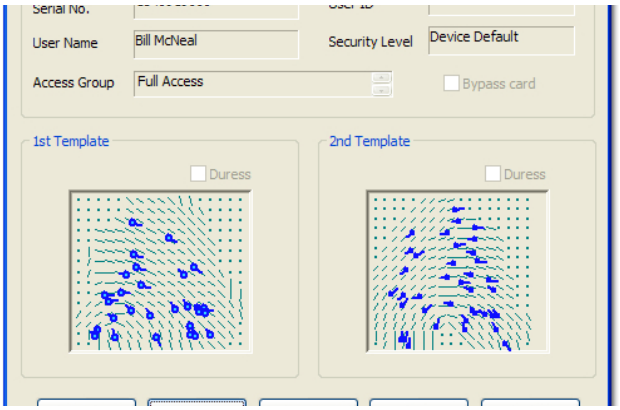
3.6.4.5 Issue MIFARE, DESFire or iCLASS template cards

MIFARE, DESFire and iCLASS template cards allow you to store user information and fingerprint templates directly on the card.

Attention: DESFire template cards can be issued with a 2.x device only.

To register a card for a user:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. In the User pane, click the Card tab.
4. Select "Mifare/DESFire Template" or "iCLASS Template" from the drop-down list.
5. Click **Card Management**. This will open the **Card Management** dialog box.



6. Select a Device ID or USB MIFARE device (if connected) from the drop-down list.

7. If desired, click Bypass Card to allow the user to bypass the fingerprint authentication.
8. Click **Read Card**. The LED on the device that you selected will begin flashing.
9. Place the card on the device.
10. After the card is read, click **OK**.
11. Click **Apply** to issue the card to the user's account.

Note: iCLASS 2000, 2002 and 2004 cards are not supported as template cards.

3.6.4.6 Change the MIFARE, DESFire or iCLASS site key

Data encryption for MIFARE, DESFire and iCLASS cards is governed by a 48-bit site key. Only those cards with appropriate site keys can be read by connected devices. BioStar allows you to define up to two MIFARE, DESFire and iCLASS site keys (primary and secondary), so that you can change the site key for existing cards.

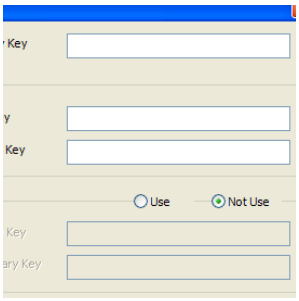
Note: This feature is only supported for template-on-cards. Also, please note that site keys must be carefully guarded. If the site key is revealed, your security system can be bypassed.

Attention: Use numbers for the site key.

Attention: DESFire site keys can be applied to only 2.x devices.

To change the site key:

1. From the menu bar, click **Option > Card > Mifare Card or DESFire Card or iCLASS Card > Mifare Sitekey or DESFire Sitekey or iCLASS Sitekey** . This will open the **Mifare Sitekey**, **DESFire Sitekey** or **iCLASS Sitekey** dialog box.



2. Enter a new primary key in the *New Primary Key* field.
3. Enter the key again in the *Retype Primary Key* field.
4. Click the *Use* option button to activate the secondary key function. This allows cards with the old site key to be read and rewritten with the new key:
   a. Enter the old site key in the *New Secondary Key* field.
   b. Enter the old site key again in the *Retype Secondary Key* field.
5. When you are finished editing the site key, click **OK**.

Note: When all cards have been rewritten with the new site key, Suprema advises disabling the secondary key function to prevent old cards from being used for access.

3.6.4.7 Edit the MIFARE layout

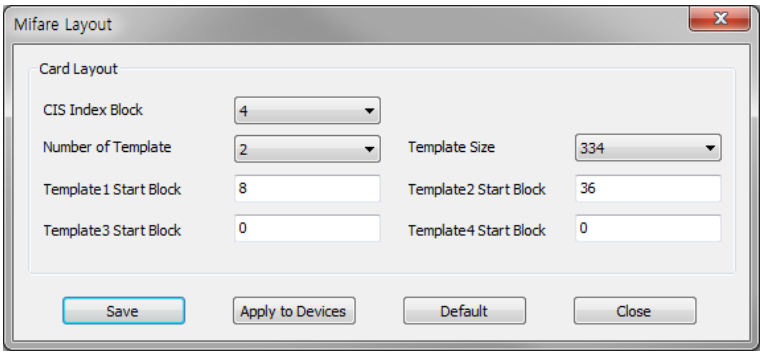
BioStar allows you to customize the layout that is used to record user information and fingerprint templates. This layout will be applied to all new MIFARE cards issued with the devices you specify.

MIFARE 1K cards are organized into 16 sectors with 4 blocks of 16 bytes each. MIFARE 4K cards are organized into 32 sectors with 4 blocks and 8 sectors with 16 blocks. The following constraints apply to the MIFARE layout:

- The first sector (block 0 through block 3) is reserved and cannot be used for other data.
- The last block of each sector (blocks 3, 7, 11, and so on) is reserved for site key information.
- The card information sector (CIS) occupies three contiguous blocks and should start at the first available block of a sector (blocks 4, 8, 12, and so on).
- There should be no overlap between each template's data.

To edit the MIFARE layout:

1. From the menu bar, click **Option > Card > Mifare Card > Mifare Layout**. This will open the **Mifare Layout** dialog box.



2. Use the drop-down lists and input fields to configure the following parameters of the MIFARE layout:
   - **CIS Index Block**: Select the block index to use for header information (*4*, *8*, *12*, or *16*).
   - **Number of Templates**: Select the number of templates to include in the layout (*0* to *4*).
   - **Template Size**: Select the number of bytes to use in the template. The default size is 334 bytes.

- **Template 1-4 Start Block**: Enter the starting block for each fingerprint template.

3. To use the custom layout, click **Apply to Devices** and select the appropriate device numbers from the **Device Tree** dialog box.
4. To save your changes, click **Save**.

Note: To reset any changes you have made, click **Default**. To exit the dialog box without saving changes, click **Close**.

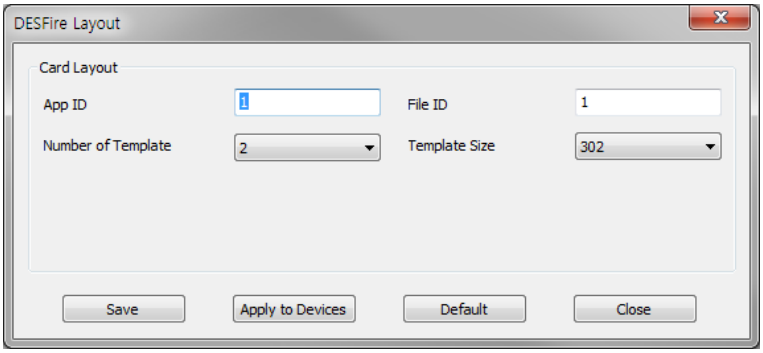
3.6.4.8 Edit the DESFire layout

BioStar allows you to customize the layout that is used to record user information and fingerprint templates. This layout will be applied to all new DESFire cards issued with the devices you specify.

Attention: DESFire site keys can be applied to only 2.x devices.

To edit the DESFire layout:

1. From the menu bar, click **Option > DESFire Card > DESFire Layout**. This will open the **DESFire Layout** dialog box.



2. Enter the following parameters of the DESFire layout:
   - **App ID**: Set the application ID. This plays a role of directory which includes file ID.
   - **File ID**: Set the file ID.
   - **Number of Templates**: Select the number of templates to include in the layout (*default is 2*).
   - **Template Size**: Select the number of bytes to use in the template. The default size is 302 bytes.
3. To use the custom layout, click **Apply to Devices** and select the appropriate device numbers from the **Device Tree** dialog box.
4. To save your changes, click **Save**.

Note: To reset any changes you have made, click **Default**. To exit the dialog box without saving changes, click **Close**.

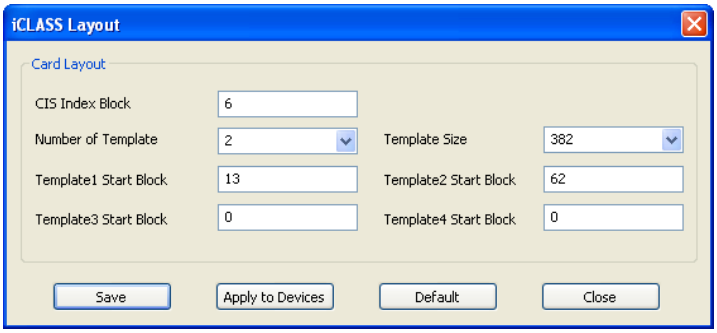
3.6.4.9 Edit the iCLASS layout

BioStar allows you to customize the layout that is used to record user information and fingerprint templates. This layout will be applied to all new iCLASS cards issued with iCLASS devices.

BioEntry Plus iCLASS devices support 16k bit (2k Byte) and 32k bit (4k Byte) iCLASS cards. The 16k bit (2k Byte) cards are available with either 2 or 16 application areas and are organized into 237 blocks of 8 bytes each. The 32k bit (4k Byte) cards are available with either 2 or 16 application areas, plus an additional 16k user configurable memory, and are organized into 8 pages with 26 blocks of 8 bytes each.

To edit the iCLASS layout:

1. From the menu bar, click **Option > iCLASS Card > iCLASS Layout**. This will open the **iCLASS Layout** dialog box.

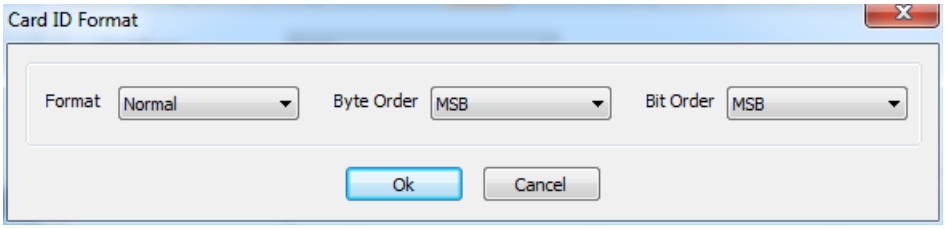


2. Enter the following parameters of the iCLASS layout:
   - **CIS Index Block**: Select the block index to use for header information (*default value is 13*).
   - **Number of Templates**: Select the number of templates to include in the layout (*default is 2*).
   - **Template Size**: Select the number of bytes to use in the template. The default size is 382 bytes.
   - **Template 1-4 Start Block**: Enter the starting block for each fingerprint template (Template 1 default value is 19; Template 2 default value is 67).
3. To use the custom layout, click **Apply to Devices** and select the appropriate device numbers from the **Device Tree** dialog box.
4. To save your changes, click **Save**.

Note: To reset any changes you have made, click **Default**. To exit the dialog box without saving changes, click **Close**.

3.6.4.10 Read card information from USB-based readers

You can specify options to read information from USB-based contactless readers like a DE-620 by clicking **Option** > **Card** > **USB Reader** > **Card ID Format**.



- **Format**: Set the type of pre-processing on the card ID data to Normal, allowing the data to be processed in its original form. Wiegand type is not supported.
- **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (MSB) or least significant byte (LSB).
- **Bit Order**: Specify whether to swap ID card data between cards and devices by most significant bit (MSB) or least significant bit (LSB).

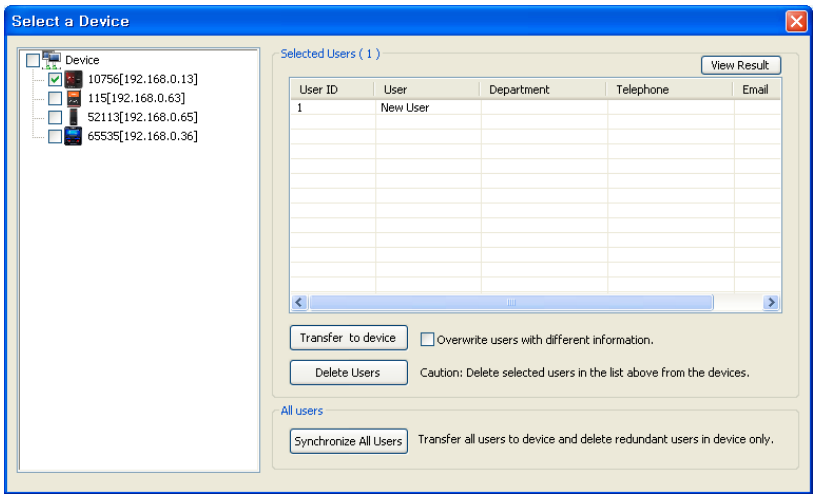
3.6.5 Transfer User Data

BioStar allows you to automatically transfer user information to devices, by selecting the "Auto" setting from the menu bar (**Option > User > Transfer Mode > Auto**). However, you can also manually transfer data to devices. When doing so, you can either transfer selected users to selected devices or synchronize all users at once. BioStar also allows you to retrieve data from a device and transfer it to the BioStar server.

3.6.5.1 Transfer a user to a device

To transfer a single user or selected users to a device or devices:

1. Click **User** in the shortcut pane.
2. In the task pane, click **Transfer Users to Device**. This will open the **Select a Device** dialog box.



3. Select a device or devices from the list on the left by clicking the checkboxes next to device names.
4. If desired, click the checkbox to overwrite users with different information.
5. Click **Transfer to Device** to send the user information to the selected devices.

Note: You can also delete users from devices with this menu. This action cannot be undone, so use this feature with caution. To delete users from a device, click a user's name and then click **Delete Users**.

When using Xpass or Xpass S2 devices as lift readers, transferring settings to the device with the User menu will reset all of the settings and user data stored on the device. To preserve the settings, use the *Transfer to Device* function in the Lift menu instead.

3.6.5.2 Synchronize all users

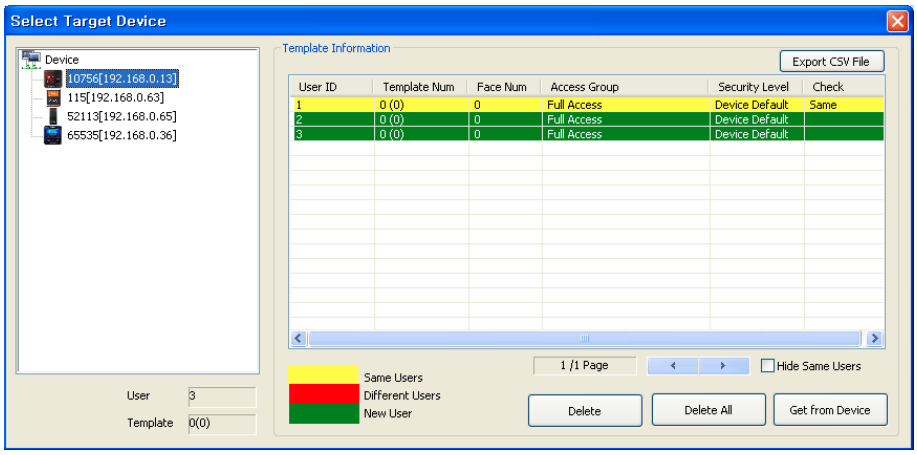
To synchronize all user information between the BioStar server and connected devices,

1. Click **User** in the shortcut pane.
2. In the task pane, click **Transfer Users to Device**. This will open the **Select a Device** dialog box (see section 3.6.5.1).
3. Select a device or devices from the list on the left by clicking the checkboxes next to device names.
4. Click **Synchronize All Users**.

3.6.5.3 Retrieve user data from a device

To retrieve data from a device:

1. Click **User** in the shortcut pane.
2. In the task pane, click **Manage Users in Device**. This will open the **Select Target Device** dialog box.



3. Click a device name in the list on the left to display user templates contained in the device.
4. Click a user in the Template Information list (new users will be highlighted in yellow).
5. Click **Get From Device**.

Note: You can also delete users from devices with this menu. This action cannot be undone, so use this feature with caution. To delete users from a device, click a user's name and then click **Delete** (or click **Delete All** to delete all user records at once).

In the template information, "Template Num" is the number of fingerprint templates stored in the device and "Face Num" is the number of face templates stored in the device.

Caution: If there are the same users on the BioStar database when you retrieve user data from Xpass devices, the data will be overwritten without fingerprint data because Xpass devices do not store fingerprint data.

Caution: Department information and PIN cannot be imported when importing user information saved in BioStation 2, BioStation A2 or BioStation L2.

3.6.5.4 Merge user data imported from the device

This is to protect the existing data in the server, but import only changed or added user data from the device. If you choose 'Overwrite', this will delete the entire user data previously saved and replace with the user data imported from the device.

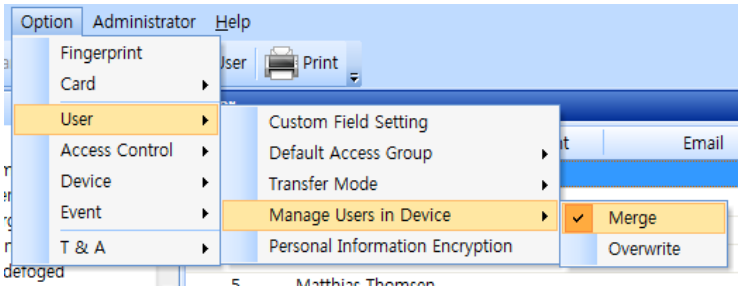
To protect important user data, the following 5 items will not be merged and saved to the server DB.

- Admin Level (Changed only if admin level is 'Normal User' in the server database and 'Admin User' in the device.)
- Authentication mode
- Number of Authentication
- Authentication time limit

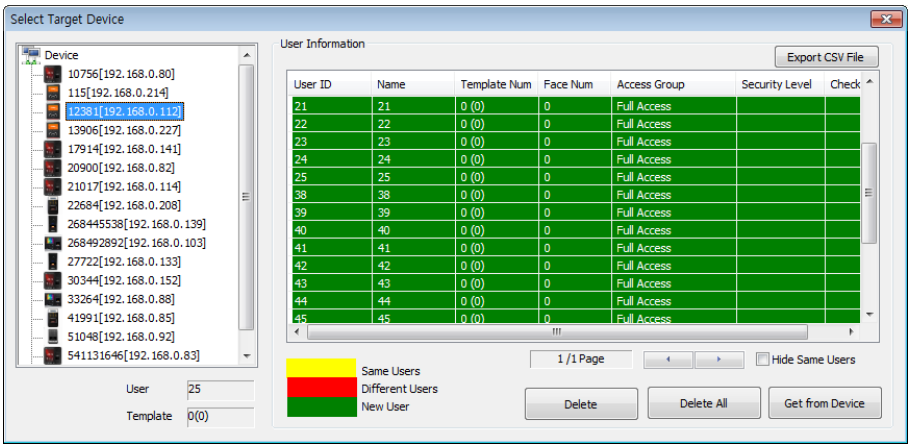
- Password

Merge and import user data

1. Click Option > User > Manage Users in Device. Check the Merge option. (Default)



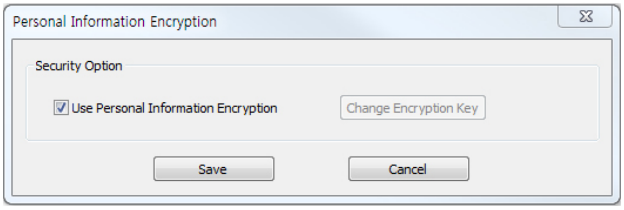
2. In the shortcut pane, click User.
3. In the task pane, click Manage Users in Device. This will open the Manage Users in Device window.



4. Click the device name in the device list on the left and display user information in the device.
5. With color information, compare user data between the device and server and select users.
6. Click Get from Device.

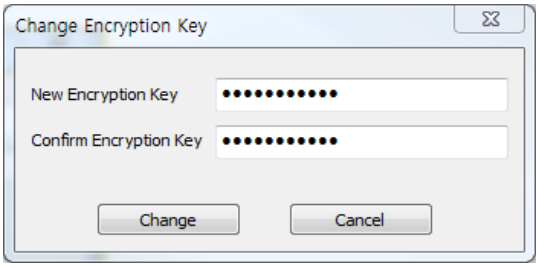
3.6.6 User Data Encryption

BioStar provides AES256 user data encryption. User data encryption helps protect valuable private information against crimes such as identity theft upon any accidental or intentional data breach.



To encrypt user data:

1. Click **Option** > **User** > **Personal Information Encryption**.
2. In the **Personal Information Encryption** dialog box, click the check box beside **Use Personal Information Encryption** – a pop-up window will appear.
3. Read the message then click **Yes** to accept it.
4. Click **Change Encryption Key** then enter the encryption key.



Note You can use Personal Information Encryption without encryption keys. Any combination of letters, numbers and special characters up to 32 characters can be used as the encryption key.

5. Click **Change** to close the window then click **Save** to save changes.

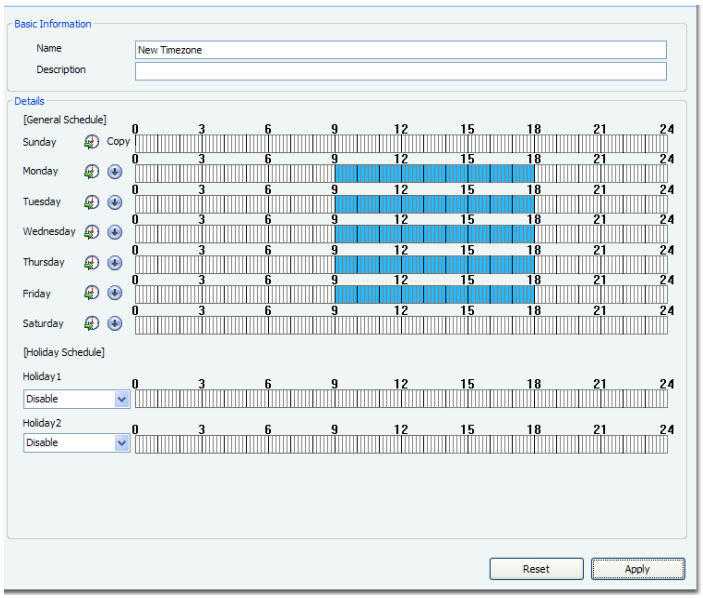
3.7 Setup Timezones

In the BioStar system, timezones are used to schedule permissions and restrictions. You can apply timezones to restrict the hours that a user is permitted to access a door by combining doors and timezones in access groups (see section 3.8).

3.7.1 Create a Timezone

To create a timezone schedule:

1. Click **Access Control** in the shortcut pane.
2. In the task pane, click *New Timezone*.
3. Enter a name for the timezone.
4. In the Timezone pane, create a weekly schedule by highlighting the effective hours for each day. You can copy a schedule from one day to the next by clicking the arrow to the right of the day.



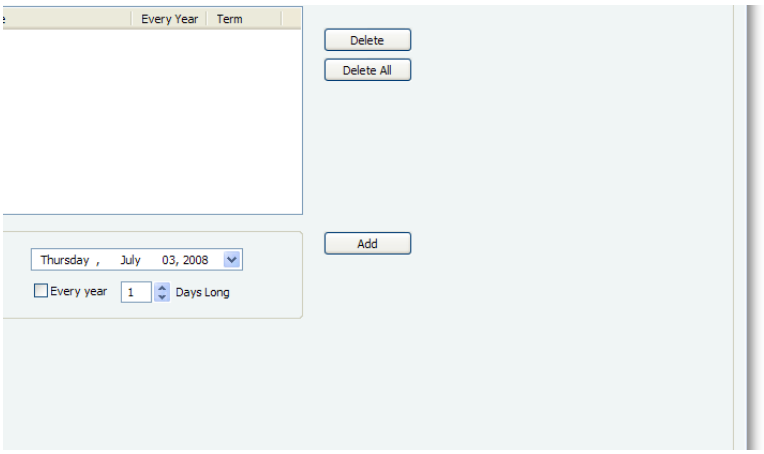
5. If desired, you can add up to two holiday schedules to the timezone. To create holiday schedules, see section 3.7.2.
6. When you are finished creating the timezone, click **Apply**.
7. Next, transfer the timezone data to devices:
8. In the task pane, click **Transfer to Device**. This will open the **Device Tree** dialog box.
9. Select a device or devices by clicking the checkboxes in the **Device Tree** dialog box.
10. Click **OK**.

You can now combine the timezone with door permissions to create an access group (see section 3.8).

3.7.2 Create a Holiday Schedule

To create a holiday schedule:

1. Click **Access Control** in the shortcut pane.
2. In the task pane, click **New Holiday**.
3. Enter a name for the holiday.
4. In the Holiday pane, set the date the holiday begins with the drop-down calendar.



5. If the holiday recurs every year, click the checkbox below the drop-down list.
6. Set the duration of the holiday (in days).
7. Click **Add** to add the holiday to the list.
8. Click **Apply**.

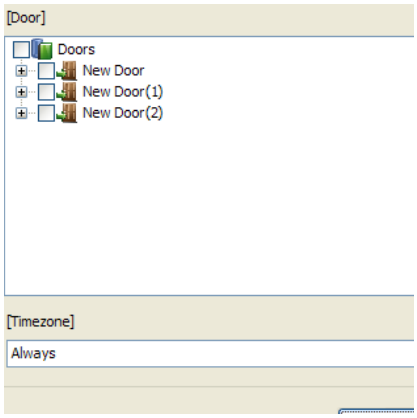
3.8 Setup Access Groups

Access groups allow you to define sets of access permissions that can include doors, users, and timezones. Before adding an access group, you must setup doors (see section 3.3) and timezones (see section 3.7). After creating access groups, you must manually transfer the data to affected devices (see section 3.8.4).

3.8.1 Add an Access Group

To add an access group:

1. Click **Access Control** in the shortcut pane.
2. In the task pane, click **New Access Group**.
3. Type a name for the new access group in the box that appears in the navigation pane and press Enter.
4. In the Access Control tab (in the Access Group pane), click **Add**. This will open the **Access Group** dialog box.



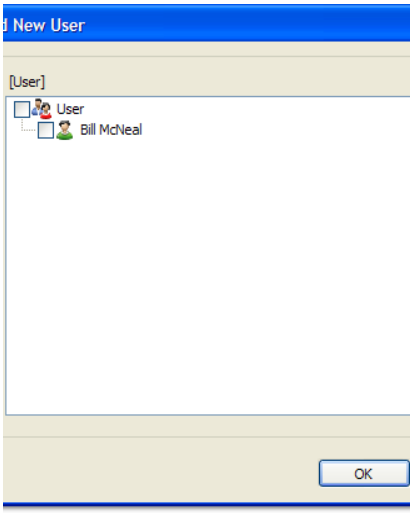
5. Select doors to add to the group by clicking the checkboxes next to door groups or individual doors.
6. Select a timezone to apply to the group from the drop-down list at the bottom of the dialog box.
7. Repeat steps 5 and 6 as necessary to add multiple sets of doors and timezones to the access group.
8. Click **OK** to add your selections to the group.

3.8.2 Add Users to Access Groups

After adding access group, you must add users to the group. You can add users to access groups from the User tab, as described below or by assigning access groups to a user from the User pane, as described in 3.8.3. You can assign a user to a maximum of four access groups.

To add users to access groups:

1. Click **Access Control** in the shortcut pane.
2. From the User tab (in the Access Group pane), click **Add**.
3. In the **Add New User** dialog box, select users to add to the group by checking user groups or individual users.



4. Click **OK**.

If you have setup user groups, users will appear under their respective groups.

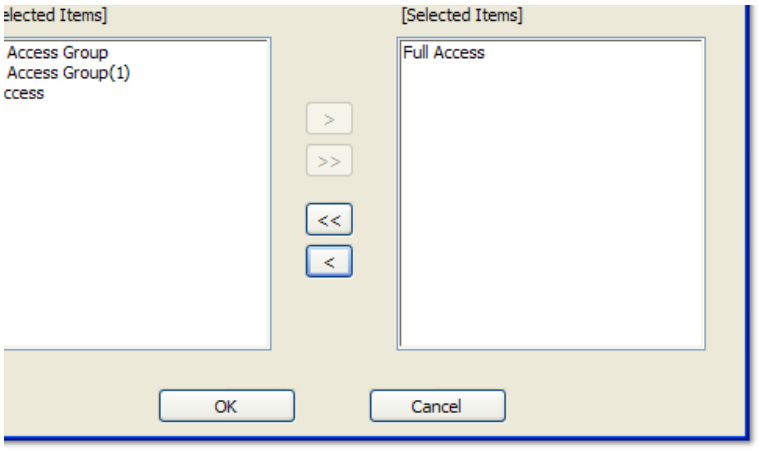
3.8.3 Assign Access Groups to Users

You can also define which access groups a user will belong to (up to four total) from the User pane.

To assign an access group to a user:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user's name.
3. Click the Access Control tab in the User pane.

4. Click **Add**. This will open the **User Access Group** dialog box.



5. Click the name of an access group from the list on the left and then click **>**.
6. Repeat step 5 as needed to assign additional access groups.
7. When you are finished assigning access groups, click **OK**.

3.8.4 Transfer Access Groups to Devices

To transfer access group data to devices:

1. Click **Access Control** in the shortcut pane.
2. In the task pane, click **Transfer to Device**. This will open the **Device Tree** dialog box.
3. Select a device or devices by clicking the checkboxes in the **Device Tree** dialog box.
4. Click **OK**.

3.8.5 Check for Access Rules by Device

You can check the access rules applied for devices by viewing access groups, timezone, and holiday schedules by device. You can also maintain the idential configuration data across the server and devices by either transferring or deleting the data that is inconsistent between them.

To check access groups configured in each device:

1. Click **Access Control** in the shortcut pane.
2. In the task pane, click **Manage Access Group in Device**. This will open the **Device Tree** dialog box.
3. Select a device in the Device tree pane.
4. Select **Access Group**, **Timezone**, or **Hoilday Schedule** below the Device tree pane to view how they are configured in each device. The configuration data to the corresponding options will be displayed in the right pane. The data will be highlited in the following colors depending on whether they are applied in the server, a device, or both.
   - **Yellow**: Indicates that the configuration data in both the device and the server are identical.
   - **Red**: Indicates that the configuration data in the device and the server are different.
   - **Green**: Indicates that the configuration data are applied to the device only.
   - **Blue**: Indicates that the configuration data are applied to the server only.
5. Optional: Select the data that you want to delete from the device and click **Delete from Device** in the lower-right corner of the screen.
6. Optional: Select the data that you want to transfer from the server to a device and click **Send to Device** in the lower-right corner of the screen.

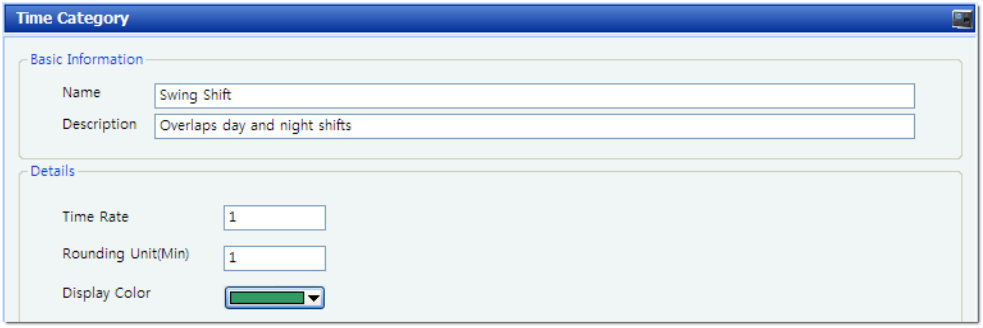
3.9 Setup Time and Attendance

BioStar's time and attendance features allow you to define time categories, shifts, and holiday rules. Refer to the procedures in this section as well as the steps in section 3.7.2 to configure time and attendance options.

3.9.1 Add a Time Category

To add a time category:

1. Click **Time and Attendance** in the shortcut pane.
2. In the task pane, click **Add Time Category**. This will open a Time Category pane similar to the one below.



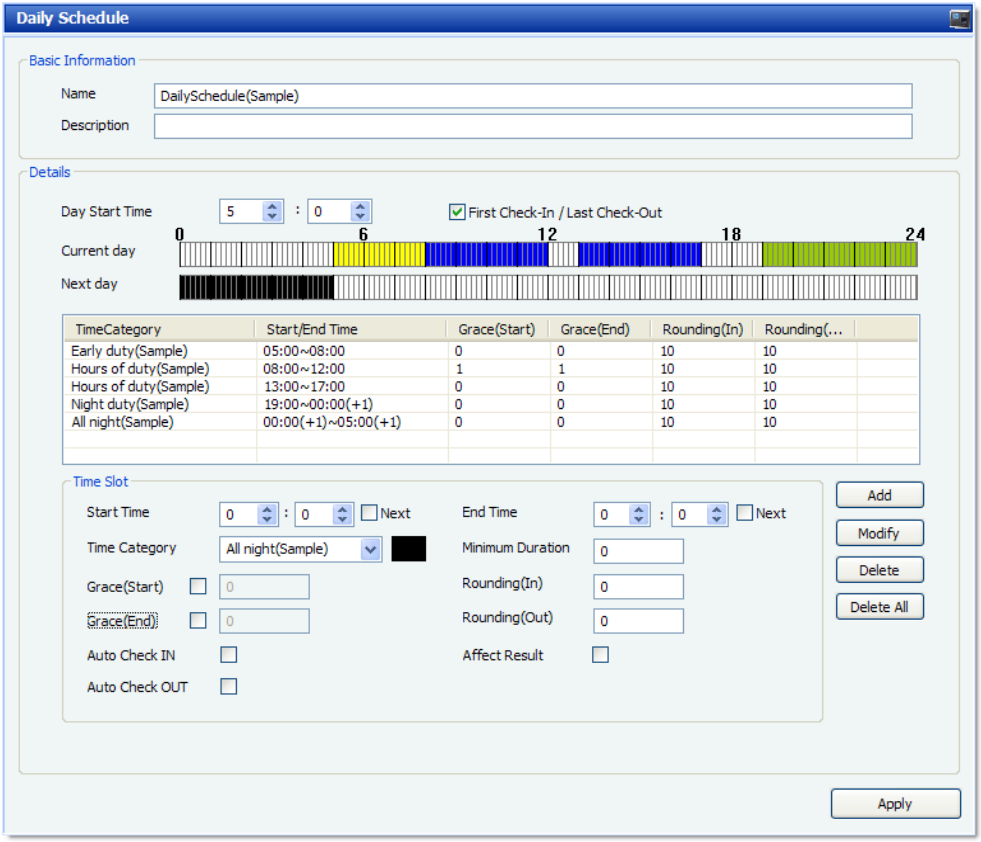
3. Enter a name and description for the time category.
4. Add details for the time category:
   - **Time Rate**: Enter the rate at which time is calculated for this time category.
   - **Rounding Unit(Min)**: Specify in minutes how to round a user's work time (for example, a entry of "5" will round a user's work time to the nearest 5-minute decrement).
   - **Display Color**: Set how the time category will appear in the daily schedule.
5. Click **Apply** to save the time category.

3.9.2 Add a Daily Schedule

BioStar versions 1.35 and higher support a maximum of 256 daily schedules.

To add a daily schedule:

1. Click **Time and Attendance** in the shortcut pane.
2. In the task pane, click **Add Daily Schedule**. This will open a Daily Schedule pane similar to the one below.



3. Enter a name and description for the daily schedule.

4. Set the start time for the daily schedule and, if desired, click the checkbox to the right to let the BioStar to record workers' first come-in and last go-out activities via the BioStar system as their check-in and check-out activities for the day.

5. Define the daily schedule by adding one or more time slots:

   b. Specify the details for the time slot:

   - **Start time**: Set the beginning time for the time slot. If the time slot begins in the following calendar day, click the checkbox ("Next") to the right.
   - **End time:** set the ending time for the time slot. If the time slot ends in the following calendar day, click the checkbox ("Next") to the right.
   - **Time Category**: Select one a time category from the drop-down list. See section 3.9.1 to define the time categories that will appear in this list.
   - **Minimum Duration**: Set the minimum duration for the time slot (in minutes). Workers must be checked in for at least the minimum duration, or the system will record no time worked for the time slot.
   - **Grace (Start):** Activate and set a grace period for checking in late at the beginning of the time slot (in minutes). Click the checkbox to enable the grace period and then specify the length of the grace period in the corresponding field. Workers who check in within the grace period will be considered to have checked in right at the start of the time slot.
   - **Grace (End)**: Activate and set a grace period for checking out early at the end of the time slot (in minutes). Click the checkbox to enable the grace period and then specify the length of the grace period in the corresponding field. Workers

who check out within the grace period will be considered to checked out right at the end of the time slot.

- **Rounding (In)**: Specify in minutes how to round a user's check-in time (for example, a entry of "5" will round a user's time to the nearest 5-minute decrement).
- **Rounding (Out):** Specify in minutes how to round a user's check-out time (for example, an entry of "5" will round a user's time to the nearest 5-minute decrement).
- **Auto Check IN:** Enable or disable this feature to automatically check-in a user who has failed to check-in for the time slot.
- **Auto Check OUT**: Enable or disable this feature to automatically check-out a user who has failed to check-out for the time slot.
- **Affect Result:** Allow or disallow data from this time slot to be used to determine overall time and attendance result per one daily schedule.

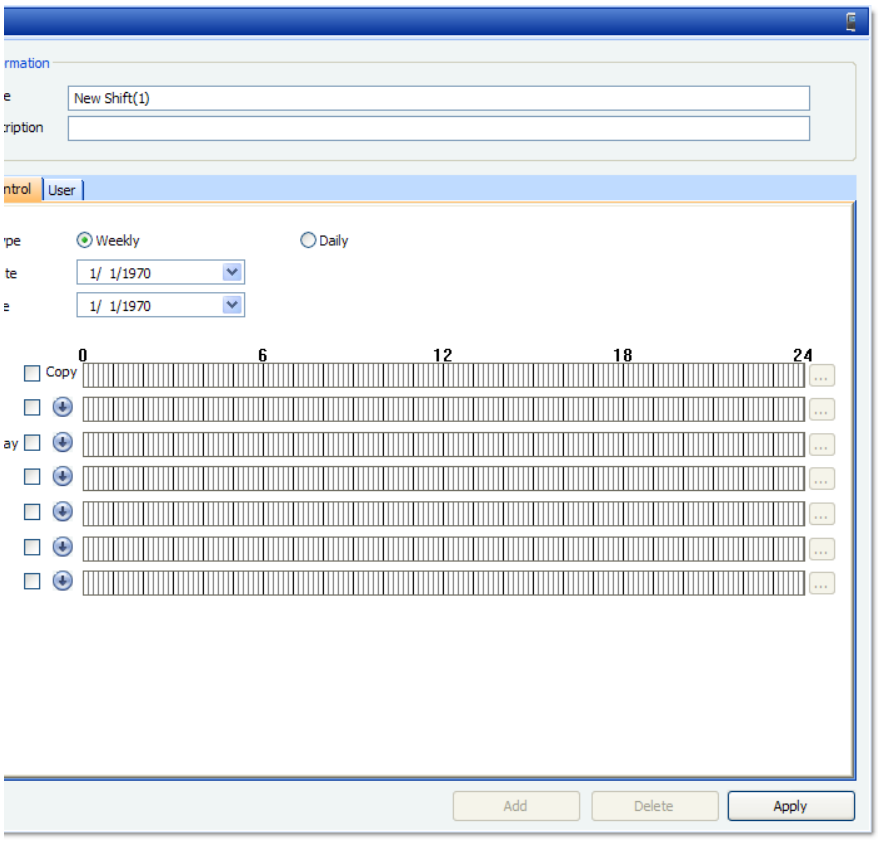
c. Click **Add** to add the time slot to the daily schedule.

6. Click **Apply** to save the daily schedule.

3.9.3 Add a Shift

To add a shift:

1. Click **Time and Attendance** in the shortcut pane.
2. In the task pane, click **Add Shift**. This will open a Shift pane similar to the one below.

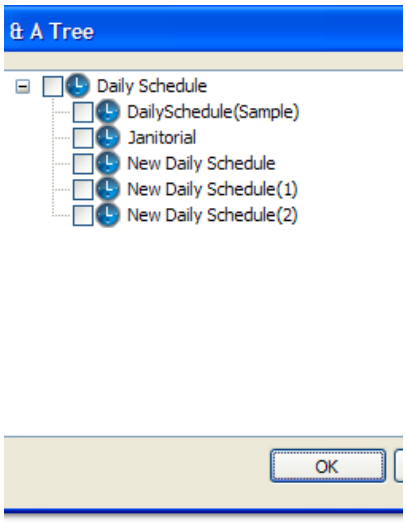


3. Click one of the option buttons to set the shift as a part of a daily or weekly cycle. If you select “weekly,” a calendar week will constitute a cycle. If you select “daily,” you can specify any number of consecutive days (e.g., 5, 10, or 20 days) to constitute a cycle.

Note: Daily cycle is available only with the Standard Edition of BioStar.

4. Select start and end dates from the drop-down calendars.
5. Activate days of the cycle by clicking the checkboxes on the left.

6. Click the ellipsis button (...) to select a daily schedule. This will open the **T&A Tree** dialog box. See section 3.9.2 to define the daily schedules that will appear in this dialog box.



7. Select a daily schedule and click **OK** to apply the daily schedule to the shift.
8. Repeat steps 5-7 as needed.

Note: You can copy a schedule from one day to the next by clicking the arrow to the right of the day. In addition, you can add up to 1,024 daily schedules to the list.

9. Click **Apply** to save the shift.

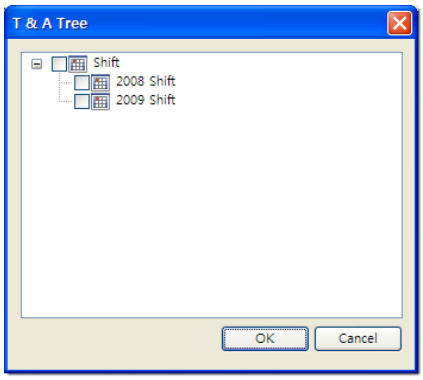
3.9.4 Assign Users to Shifts

Assign users to shifts to enable BioStar to record time and attendance data. You can assign individual users to shifts via the User pane or assign multiple users to a shift via the Time and Attendance pane.

To assign individual users to shifts via the User pane:

1. Click **User** in the shortcut pane.
2. In the navigation pane, click a user name.
3. In the User pane, click the T&A tab.

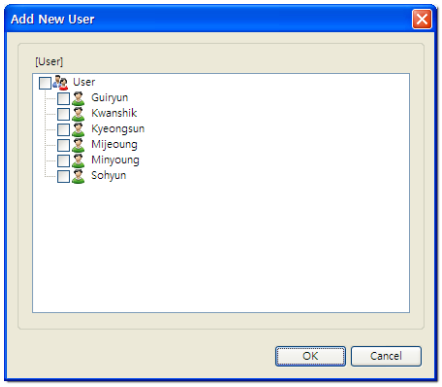
4. Click the option button next to Shift Management and then click Add at the bottom of the User pane. This will open the **T&A Tree** dialog box.



5. Select a shift and click **OK**.
6. Click **Apply** to save the T&A settings for the user.

To assign multiple users to a shift via the Time and Attendance pane:

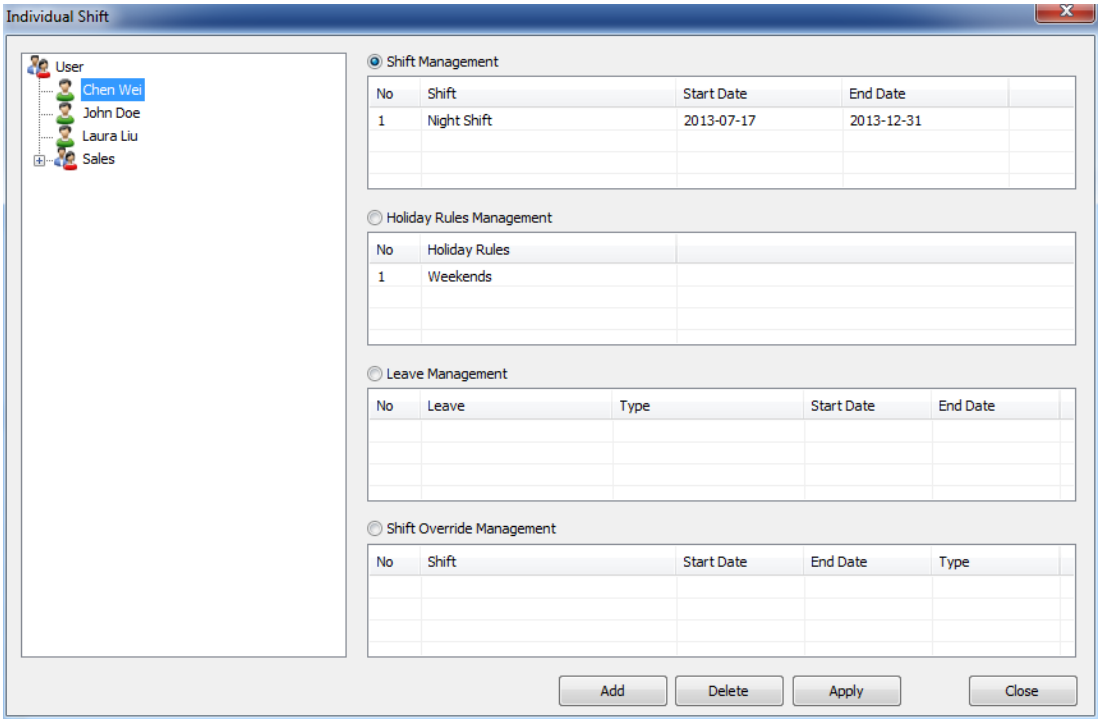
1. Click **Time and Attendance** in the shortcut pane.
2. In the navigation pane, click a shift name.
3. In the Shift pane, click the User tab and then click **Add** at the bottom of the pane. This will open the **Add New User** dialog box.



4. Select one or more users and click **OK**.
5. Click **Apply** to save the T&A settings for the shift.

To add a T& A rule by user:

1. Click **Time and Attendance** in the shortcut pane.
2. Click Individual Shift in the task pane. This will open the **Individual Shift** dialog box.



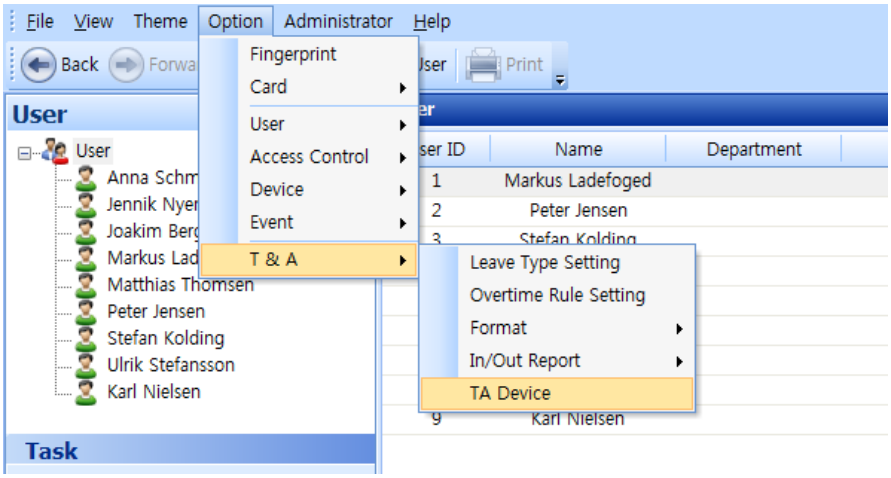
3. In the User tree pan, click the user that you want to add a T&A rule for.
4. Among the **Shift Management**, **Holiday Rules Management**, and **Leave Management**, select the appropriate option button to add a type of the schedule that you want to add, and then click **Add** in the bottom of the screen.
5. Specify the details of the schedule that you want to add, and then click OK.
6. Optional: To override the existing shift schedules, select the **Shift Override Management** option button, and then click **Add** in the bottom of the screen.

   Note: This overriden schedules are only supported for Daily Report and Individual Report when reports are created. Also, please note that they will be maintained when you choose the 'Rebuild' option, and will not be deleted even if you choose the 'Rebuild All' option.

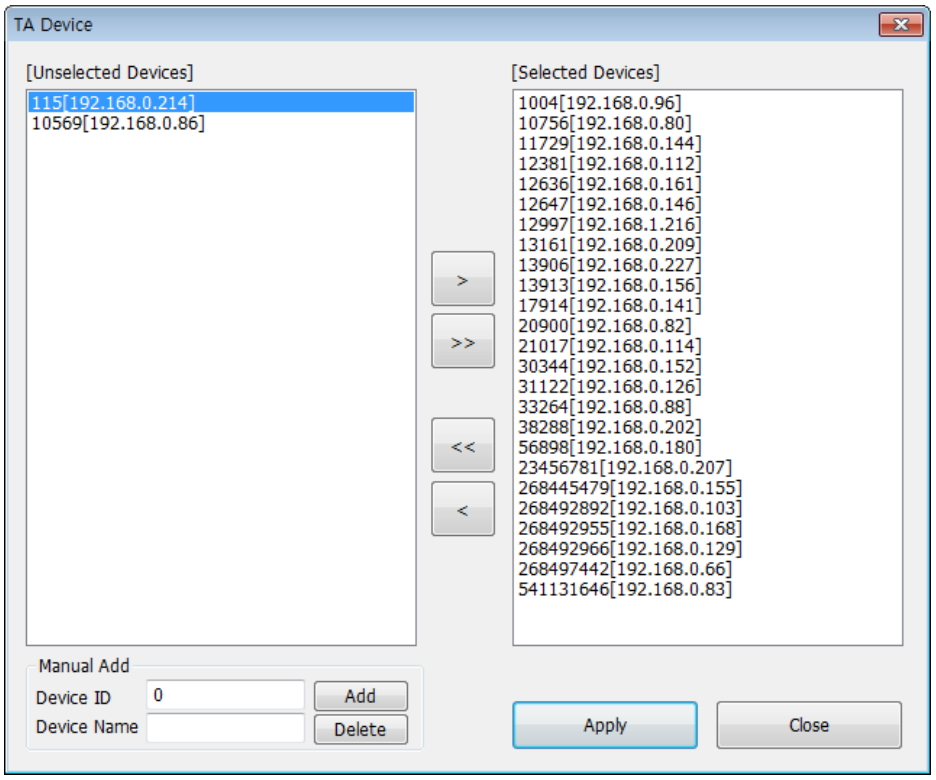
   Overriden shift schedules: Preferential shift rules which are temporarily applied
7. Specify the shift that you want to override and its period, and then click **OK**.
8. In the bottom of the screen, click **Apply** to make changes.

3.9.5 Choose a Device for T&A

Devices can be chosen for the T&A report. If Default is selected, all devices are used for T&A report. But when T&A devices are selected, T&A report is created using event logs in the selected devices. And if it is not included as a T&A device, T&A event keys applied to the device will not be displayed from the T&A report.



Select and deselect with >, >> or <, <<, and check selected devices and unselected devices through the panel. Manual Add can be made through direct device ID and name input when a device is no longer able to be found from the server but used before.



3.10 Setup Alarms

BioStar can provide multiple levels of alarm notification. The system can activate system alarms by emitting sounds from devices and connected computers. The system can also be configured to send email notifications to specified recipients. In addition, you can configure the system to receive inputs from external devices (such as fire warning devices) or send outputs to external devices (such as alarm sirens).

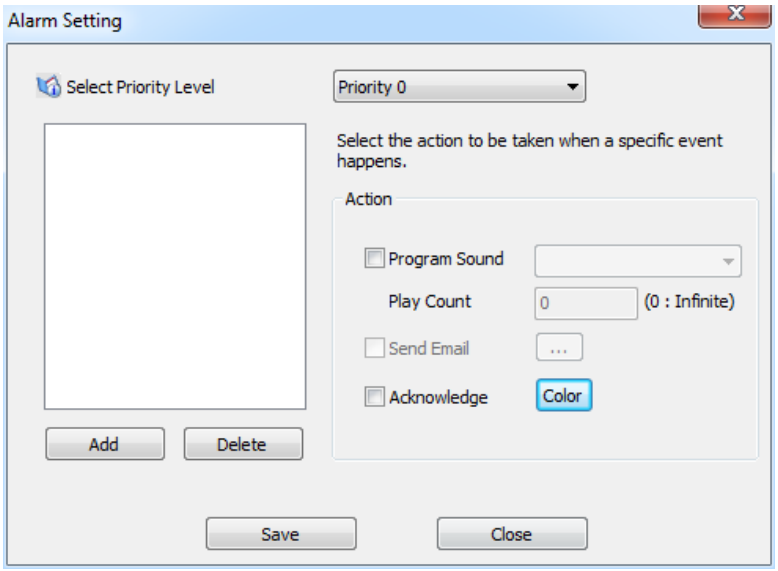
3.10.1 Configure Alarm Settings and Sounds

BioStar allows you to customize how the system responds to events. You can configure alarm settings by creating customized priority levels and selecting the action to take when an event occurs. You can also add your own alarm sounds to further customize the system.

3.10.1.1 Customize alarm actions

To customize alarm actions:

1. From the menu bar, click **Option > Event > Alarm Setting**. This will open the **Alarm Setting** dialog box.



2. Select a priority level from the drop-down list and click **Add**. This will open a list of events.
3. Select the events to include in the priority level and click **OK**.
4. Select an action or actions by clicking the checkboxes on the right.
   - **Program Sound**: Choose a sound from the drop-down list and then specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, please see section 3.10.1.2.

- **Send Email**: Click the ellipsis button (…) to the right to select an email recipient. To configure email notifications, please see section 3.10.2.
- **Acknowledge**: Activate pop-up alerts on client PCs.
- **Color**: Specify the color of text and background on any event raised by priority in the Alert Window.

5. Repeat steps 2-4 as desired to customize other priority levels.
6. When you are finished, click **Save**.

3.10.1.2 Add custom alarm sounds

To add custom alarm sounds:

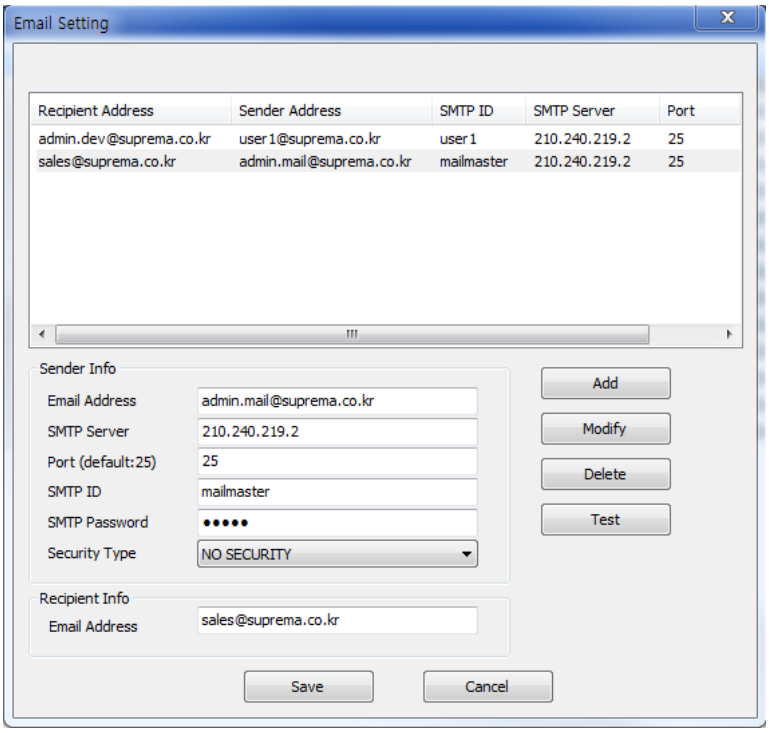
1. From the menu bar, click **Option > Event > Sound Setting**. This will open the **Sound Setting** dialog box.
2. Click **Add**.
3. Locate a waveform (.wav) file on your computer or network and click **Open**.
4. If desired, click a sound and then click **Play** to hear the sound.
5. When you are finished, click **Save**.

3.10.2 Configure email notifications

BioStar sends email notifications when an alarm event occurs (not available in the free version). As explained in 3.10.1.1, you can customize which events will trigger an automatic email alert. BioStar supports email notification through TLS or SSL secured mail servers.

To configure an email notification:

1. From the menu bar, click **Option > Event > E-mail Setting**. This will open the **Email Setting** dialog box.

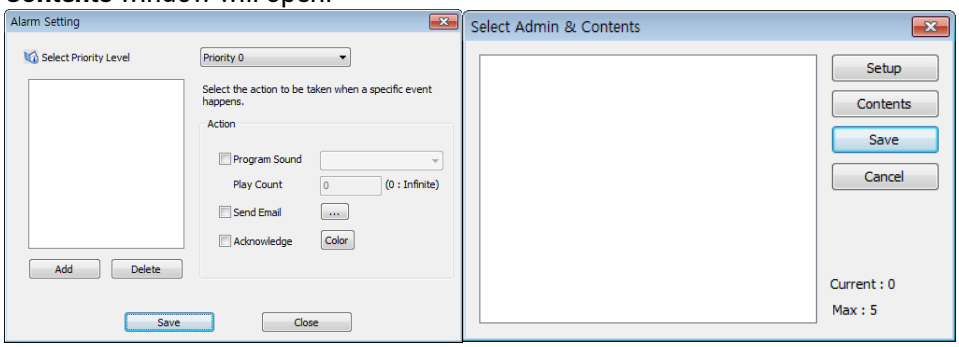


2. Type the email address, SMTP server, port number, SMTP ID, and SMTP password in the *Sender Info* section, then choose one of the options(NO SECURITY, TLS or SSL) in the Security Type drop-down list.
3. Type the email address in the *Recipient Info* section.
4. Click **Add** to add the configuration to the list.
5. Repeat steps 2-4 as necessary to add other email configurations.
6. When you are finished, click **Save**.

E-mail setting

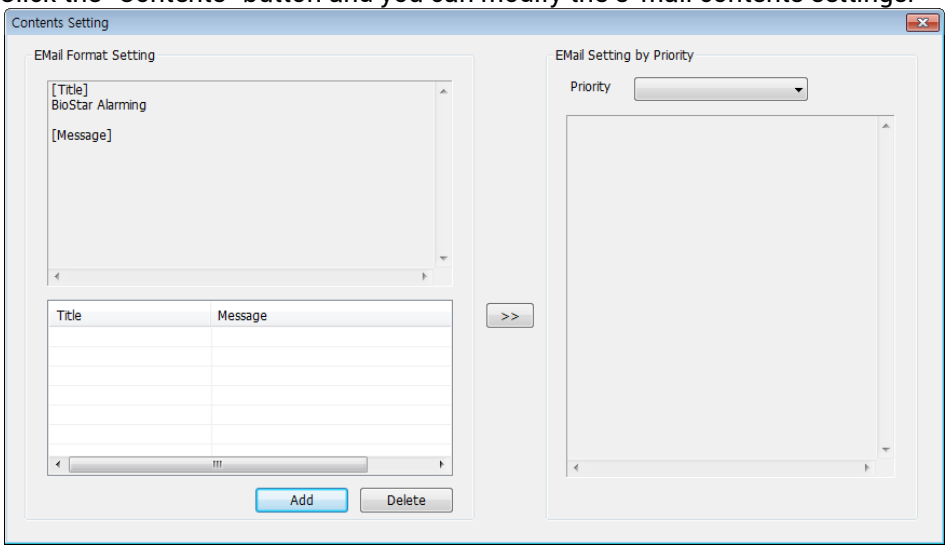
Using Alarm setting, you can send an e-mail with user-customized format.

1. Click **Option** > **Event** > **Alarm Setting** > **Send Email** > The "…" button, then the **Admin & Contents** window will open.

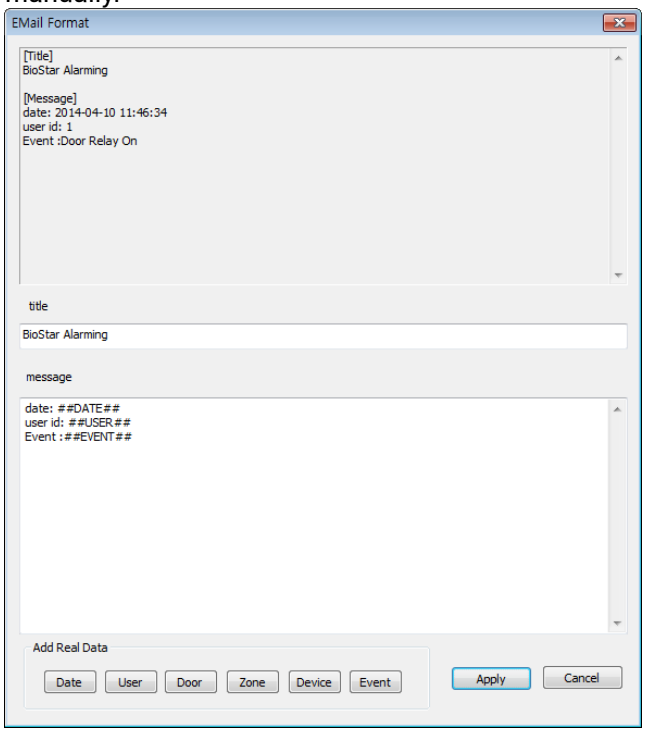


2. Click the "Setup" button and the "Email Setting" window will open.
3. Fill in "Sender Info" and click the "Add" button.

4. Click the “Add” button.
5. Click the “Contents” button and you can modify the e-mail contents settings.



6. Email contents can be applied to each Priority by using >> button.
7. Click “Add” to open “Email Format” window.
8. Select among six items in Add Real Data section to be added to Message. These items are allocated to the actual data at the designated location when email is sent out. For example, ##DATE## is changed to the actual date and time of the event, and ##USER## is changed to the actual user name. Message items can be deleted manually.



3.10.3 Configure Settings for External Devices

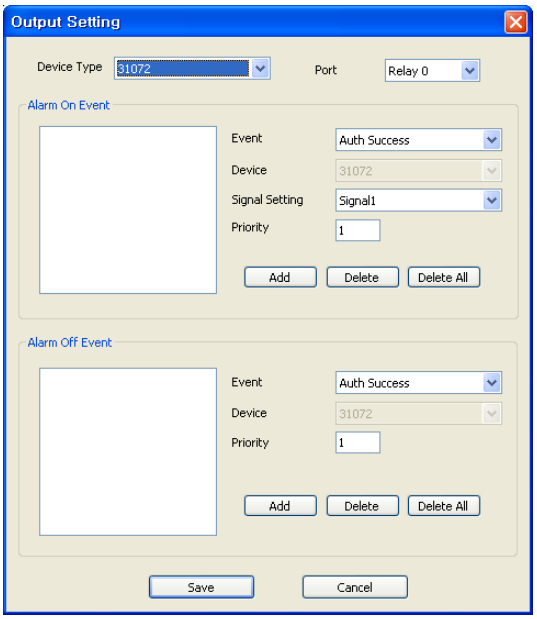
When using external devices with BioStar, you must configure settings to determine what actions will occur in response to input signals. For more information about configuring devices and device settings, see sections 3.2 and 5.1.

3.10.3.1 Configure outputs to external devices

You may choose to have certain devices send signals to external devices, such as alarm sirens, when selected events occur.

To configure outputs:

1. Click **Device** in the shortcut pane.
2. In the navigation pane, click a device name.
3. In the Device pane, click the Output tab.
4. Click **Add** at the bottom of the pane. This will open the **Output Setting** dialog box.



5. Configure actions that will activate (send a signal to) a specified output relay:
   a. In the *Alarm On Event* section, select an event from the first drop-down list.
   b. Select the device number or *All Device* from the second drop-down list.
   c. Select a signal setting from the third drop-down list.
   d. Enter a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
   e. Click **Add**.
6. Configure actions that will turn off (stop sending a signal to) an activated output relay:

a. In the *Alarm Off Event* section, select an event from the first drop-down list.
b. Select the device number or **All Device** from the second drop-down list.
c. Enter a priority for the event.
d. Click **Add**.

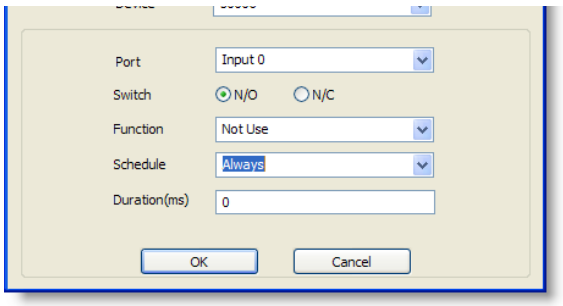
7. When you are finished, click **Save**.

3.10.3.2 Configure inputs from external devices

To integrate BioStar's door control with other alarm systems, such as fire warning systems, you can specify the actions BioStar will take when receiving an input. You can also configure inputs to work with manual door releases (exit buttons) and other types of external devices.

To configure inputs:

1. Click **Device** in the shortcut pane.
2. In the navigation pane, click a device name.
3. In the Device pane, click the Input tab.
4. Click **Add** at the bottom of the pane. This will open the **Input Setting** dialog box.



5. Select an input port from the second drop-down list.
6. Select the normal position of the input switch (*N/O-normally open* or *N/C-normally closed*).
7. Select a Function to be triggered (Generic Input, Emergency Open, Release All Alarm, Restart Device, Disable Device, LED Green Input, LED Red Input, Buzzer Input, Access Granted Input, and Access Denied Input).

   Note: With BioStar 1.8v, LED Green Input, LED Red Input, Buzzer Input, Access Granted Input, and Access Denied Input were newly added. And these input options are available only with BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), and Xpass (FW 1.3v).
8. Select a function for the input (*Not Use*, *Generic Input*, *Emergency Open*, *Release All Alarms*, *Restart Device*, or *Disable Device*).

9. Select a schedule for applying the function (*Always*, *Disable*, or custom schedules).
10. Set the minimum duration (in milliseconds) an input signal must last to trigger the specified action.
11. Click **OK**.

3.11 Setup Cameras

This section describes how to add IP cameras and network video recorder (NVR) servers to the Biostar system. Once you have properly set up the IP cameras and NVR servers, you can monitor areas in real time and view event logs with still images or recorded videos. BioStar supports the following IP cameras and NVR servers:

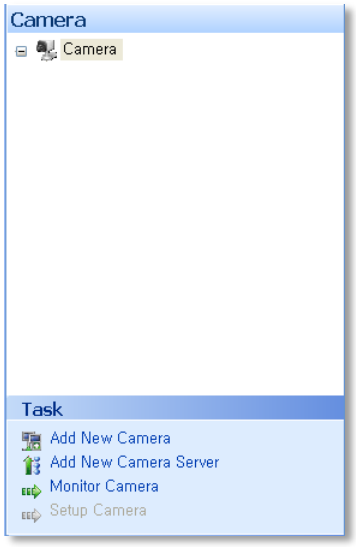
	Model Name	Developer
Internet Protocol (IP) Camera	AXIS PTZ 215	AXIS
	AXIS M3203-V	AXIS
	SNP-3120VH	Samsung Techwin
Network Video Recorder (NVR) Server	AXIS Camera Station	AXIS
	NET-I Ware	Samsung Techwin

3.11.1 Add an NVR Server

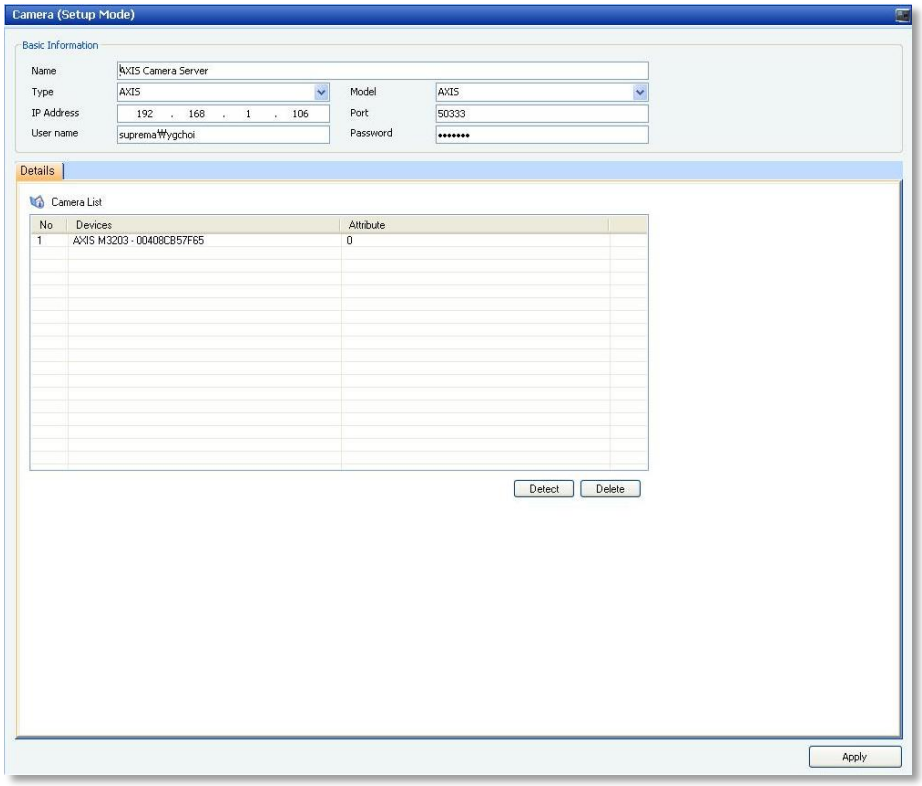
Network video recorder (NVR) servers store video streams transferred from all connected cameras and allow you to view the videos when you check event logs.

To add an NVR server to the BioStar system:

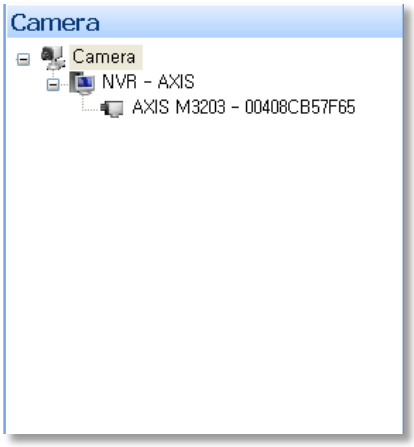
1. Click **Camera** in the shortcut pane.
2. Click **Setup Camera** in the Task pane.



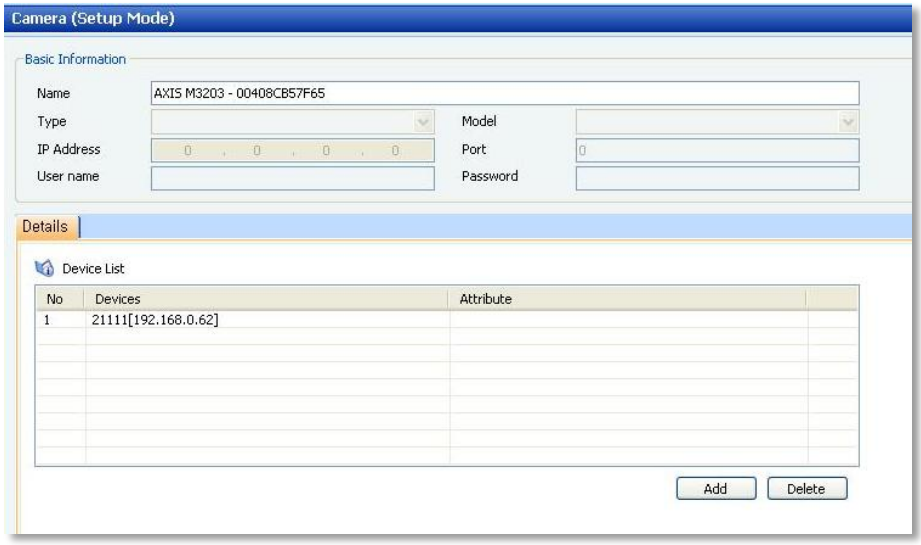
3. In the Task pane, click **Add New Camera Server**. This will open a Camera (Setup Mode) pane similar to the one below.



4. In the Basic Information section, enter a name, type, model, IP address, and port number for the NVR server, and then enter the BioStar user name and password required to access the NVR server.
5. Click **Detect** to view cameras that are currently connected to the NVR server.
6. Click **Apply** at the bottom right of the Camera (Setup Mode) pane. This will add the detected cameras under the NVR server in the navigation pane, as illustrated below.



7. In the navigation pane, click a camera name. This will open the Camera (Setup Mode) pane.



8. Click **Add** at the bottom right of the Device List to open the **Device Tree** dialog box.

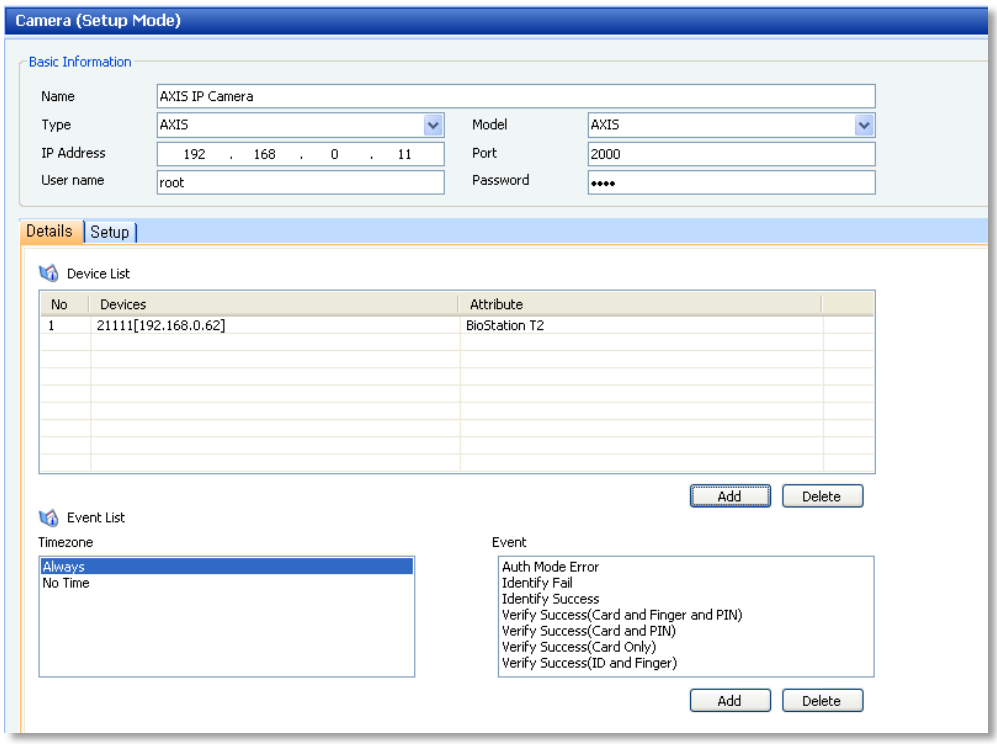
9. Click a checkbox next to a device name, and then click **OK**.
10. Click **Apply** at the bottom right to apply the changes to the BioStar system.

3.11.2 Add an IP Camera

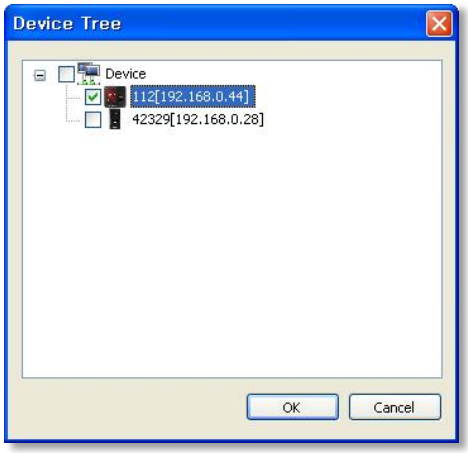
BioStar allows you to add an IP camera, assoicate it with an access control device, and specify the events that will trigger the IP camera to send captured still images to the BioStar system.

To add an IP camera to the BioStar system:

1. Click **Camera** in the shortcut pane.
2. Click **Setup Camera** in the Task pane (if desired).
3. In the Task pane, click **Add New Camera**. This will open a Camera (Setup Mode) pane similar to the one below.



4. In the Basic Information section, enter a name, type, model, IP address, and port number for the IP camera and enter a user name and password for the BioStar to acess the IP camera.
5. In the Details tab, click **Add** at the bottom right of the Device List section to open the **Device Tree** dialog box.



6. Select a device to associate the IP camera with and click **OK**.
7. Click **Add** at the bottom right of the Event List section and select an event that will trigger the IP camera to send a captured still image to the BioStar system.
8. Click **Apply** at the bottom right to apply the changes to the BioStar system.

3.11.3 Configure an IP Camera

BioStar can control the movement of pan-tilt-zoom (PTZ) cameras. When you use an IP camera that supports the PTZ feature, you can aim it at a spot you want to surveil.

To control the movement of a PTZ camera:

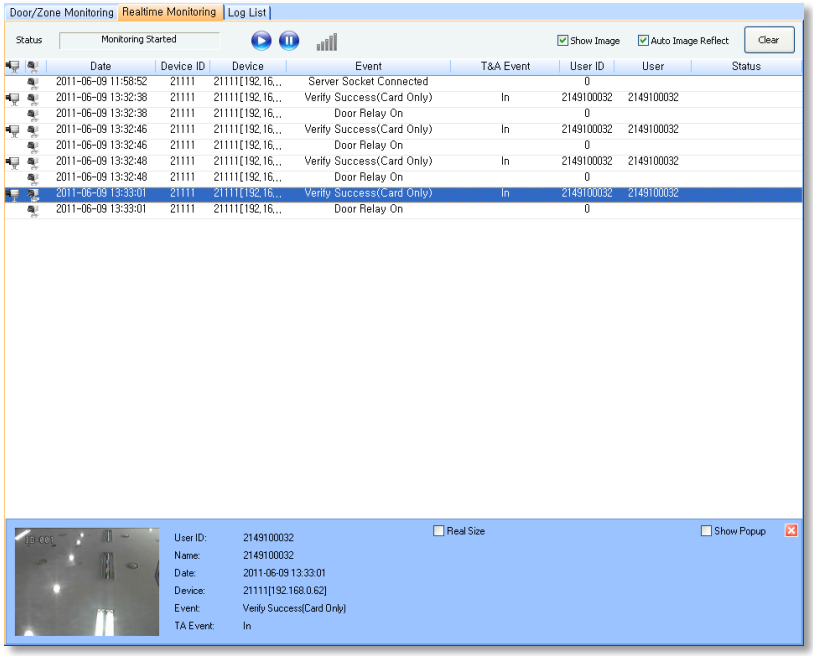
1. Click **Device** in the shortcut pane.
2. Click a PTZ camera in the navigation pane.
3. In the Camera (Setup Mode) pane, click the Setup tab.
4. Use the controls in the Pan & Tilt and the Zoom sections to aim the PTZ camera at the desired spot.

04 Manage the BioStar System

Once you have properly set up the BioStar system, management is fairly simple. BioStar allows you to monitor events in real-time and view event logs by date, control parts of the system remotely, manage users, and upgrade device firmware directly from the BioStar interface. In addition, you can activate fingerprint encryption, if necessary, to provide an additional level of security and privacy.

4.1 Monitor Events in Real Time

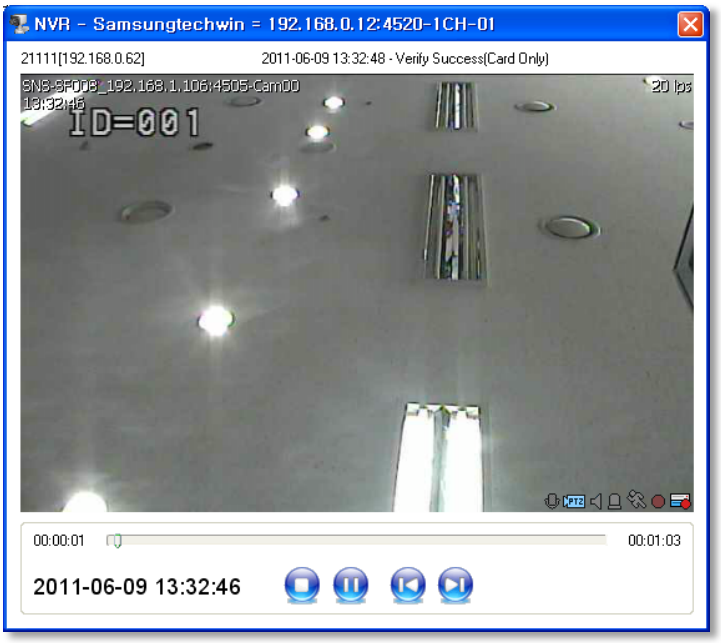
The BioStar system records events from all connected devices. To monitor events in real time, please click **Monitoring** in the shortcut pane, then click the Realtime Monitoring tab.



- This tab shows all events that have occurred since you last logged into the system. The tab shows the current monitoring status (*Monitoring Started* or *Monitoring Paused*) and includes buttons for starting (play) or stopping (pause) real-time monitoring. The sound bar icon on the right shows whether an alarm sound is currently playing (green bars) or not (grey bars). To stop an alarm sound, click the sound bars icon.
- BioStar displays the following camera icons at the front of the event logs:

Icon	Description
	The event log includes a still image. Click the event log to view the image.
	The event log includes a video. Double-click the event log to view the video.

When both camera icons are displayed, single-click the icon to view the still image and double-click the icon to view the recorded video. When you double-click the video icon, a video playback window will appear that is similar to the one below.



Coupled with the face detection features of X-Station, BioStation T2, FaceStation, or BioStation A2, administrators can verify users' identity by clicking **Show Image** (to view the user's stored face image) and **Auto Image Reflect** (to view the most recent face image captured by the local device). Clicking **Show Image** also opens a window at the bottom where the user image will be displayed. Click **Real Size** to view the full-sized (640 x 480) stored image, instead of a thumbnail version and click **Show Popup** to open the image in a new window that can be repositioned on the screen.

To see a users' photos upon successful authentication events, click **Option** > **Event** > **Profile Image Setting** in the menu bar, select event types, and then click the checkbox next to Show Image Profile. The user's image will appear on the realtime monitoring tab when he or she successfully completes one of the authentication events specified in the **Profile Image Setting** dialog box.

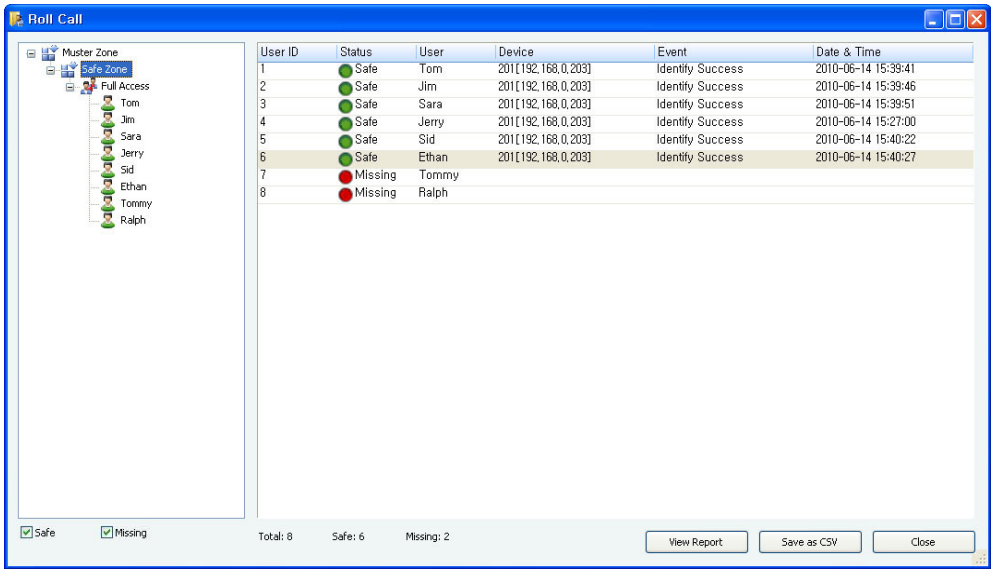
As of BioStar V1.3, administrators can monitor users' locations and authentication status via a Roll Call (muster) feature. This feature allows administrators to determine whether users are present, missing, or have gained entry to areas for which they are not authorized.

4.1.1 Monitor Muster Zones in Real Time

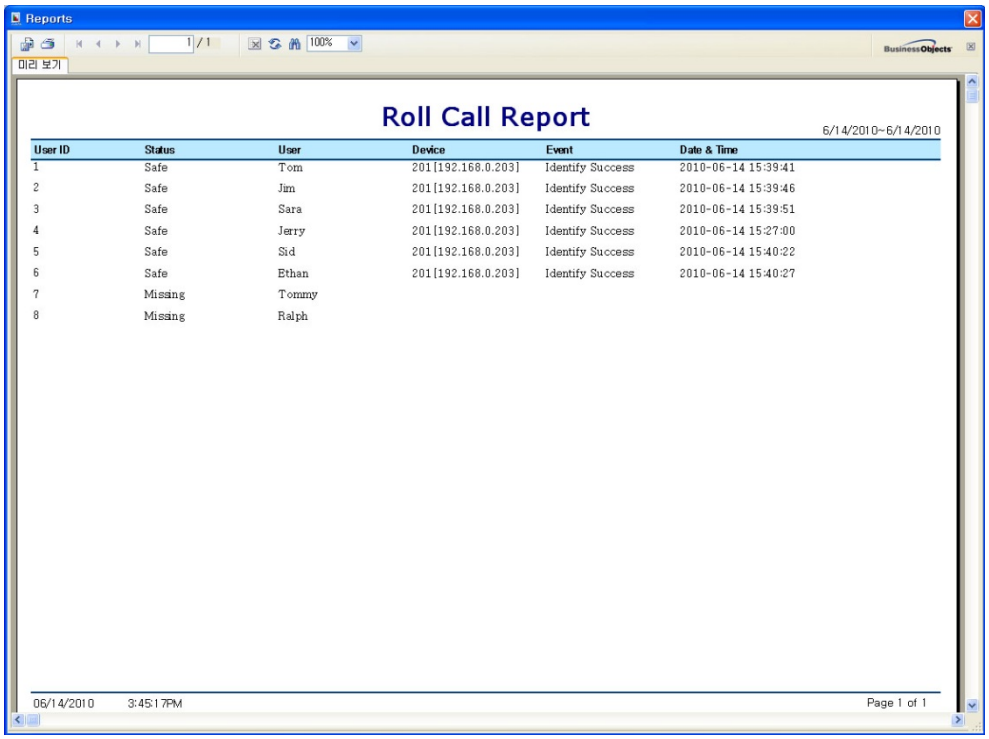
BioStar allows you to monitor and track employees during an emergency and determine whether or not all employees have reported to the muster area.

To monitor and track employees:

1. Click **Monitoring** in the shortcut pane.
2. Click a muster zone in the Monitoring pane.
3. In the Task pane, click **Roll Call**. This will open the **Roll Call** dialog box.



4. Click **View Report** to open the Roll Call Report.



To save the report data as a comma delimited file, click **Save as CSV**. To print the report, click the printer icon. To export the report, click the export icon.

4.1.2 Monitor Areas with Cameras in Real Time

BioStar allows you to monitor specified areas with the connected camera in real time.

To monitor specified areas in real time:

1. Click **Camera** in the shortcut pane.
2. Click **Monitor Camera** in the Task pane (if desired).
3. Click a camera in the navigation pane.

4.2 View Event Logs

BioStar allows you to view event logs for users, doors, and zones. You can access pre-defined logs from the Event tabs in user, door, and zone panes or view access logs from the Administrator menu. You can also use the Log List tab in the Monitoring pane to specify log parameters.

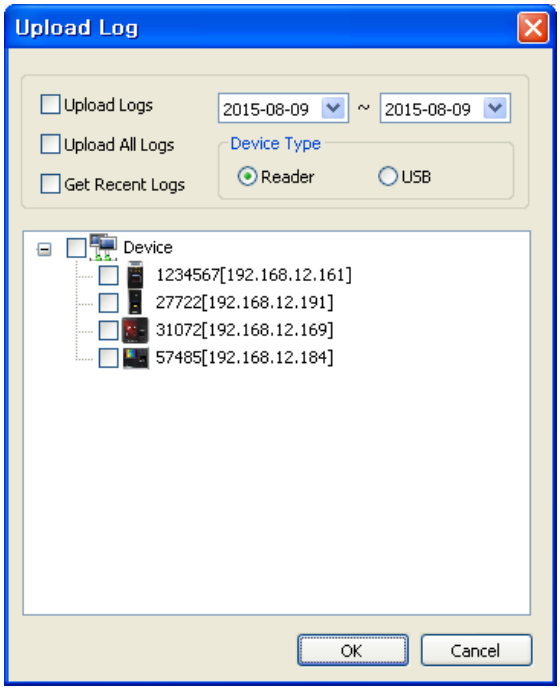
BioStar automatically collects log information from connected devices as long as the server is running. However, if you have devices that are not connected to the BioStar server, you must manually upload logs before viewing them.

4.2.1 Upload Logs to BioStar

For devices that are not connected to the BioStar server, you must manually upload logs before viewing them.

To upload logs to BioStar:

1. Click **Monitoring** in the shortcut pane.
2. Click the Log List tab in the Monitoring pane.
3. In the Task pane, click **Upload Log**. This will open the **Upload Log** dialog box.



4. Select an upload option by clicking the corresponding box:
   a. **Upload Logs**: Use this option to upload logs for a specific time period. Specify the period with the drop-down calendars.
   b. **Upload All Logs**: Use this option to upload all logs.
   c. **Get Recent Logs**: Use this option to upload logs written since the previous upload.
   d. **Device Type**: Specify a device type that you wan to upload log data from, either a reader or USB.
5. Select the devices from which to upload logs by clicking the checkboxes next to the device numbers.
6. Click **OK**. BioStar will download log records from the selected devices and display the activities in the log list.

   Note: Log upload is only supported for X-Station, BioStation T2, and FaceStation.

4.2.2 View Logs in User, Door, and Zone Panes

To view pre-defined logs:

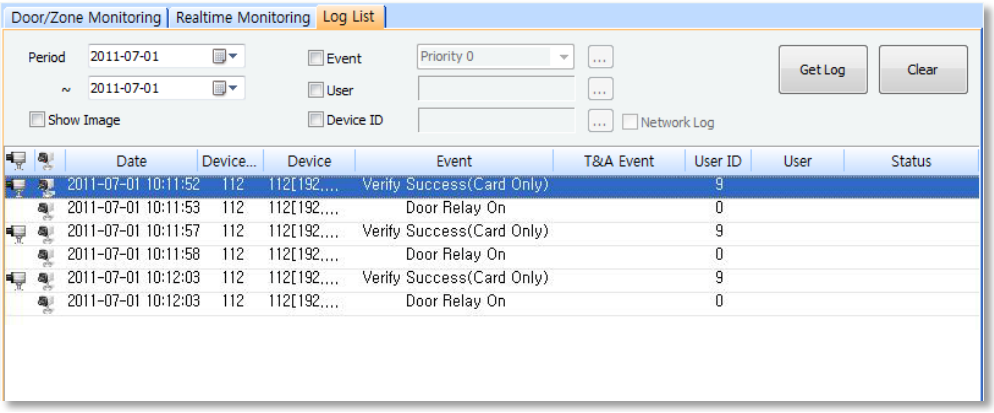
1. Click **User** or **Doors** in the shortcut pane.
2. In the navigation pane, click a user, door, or zone name.
3. In the User, Doors, or Zone panes, click the Event tab.
4. Set an event period (beginning and ending dates) with the drop-down calendars.
5. Click **Get Log**. This will generate a list of the relevant events for the period you specified.

4.2.3 View Logs from the Monitoring Pane

To specify log filters or view logs for groups of users, doors, or zones:

1. Click **Monitoring** in the shortcut pane.
2. In the Monitoring pane, click the Log List tab.
3. Set an event period (beginning and ending dates) with the drop-down calendars.
4. Set the parameters to generate a log:
   - To show events by alarm priority, click the Event checkbox and select an event priority from the drop-down list. To add a new alarm priority, click the ellipsis button (...) to open the **Alarm Priority** dialog box.
   - To show events by user, click the User checkbox and then click the ellipsis button (…) to select a user or users from the **User Tree** or **Department Tree** dialog box. You can select all users by selecting the top level of the user tree.
   - To show events for a particular device, click the Device ID checkbox and then click the ellipsis button (...) to select a device from the **Device Tree** dialog box. To show only network events for a device, you can also click the Only Network History checkbox.
   - To show all events, leave all the checkboxes unchecked.
   - To show the user's image at the bottom of the tab, click **Show Image**. For more information about viewing user images, see section 4.1.

5. Click **Get Log** to display the events.

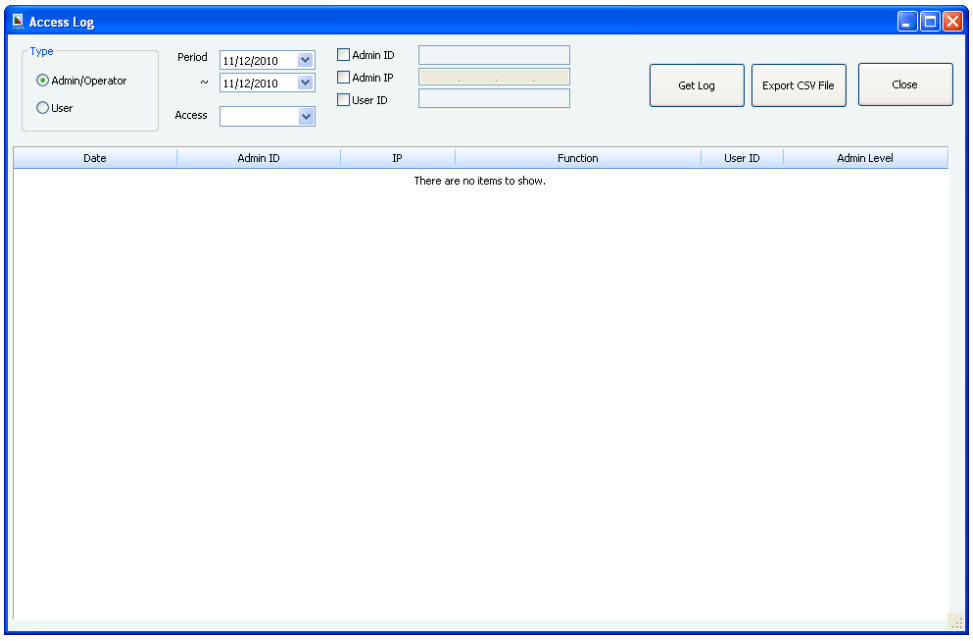


4.2.4 View Access Logs

From the Administrator menu, you can view histories of system access and record modification by type of user.

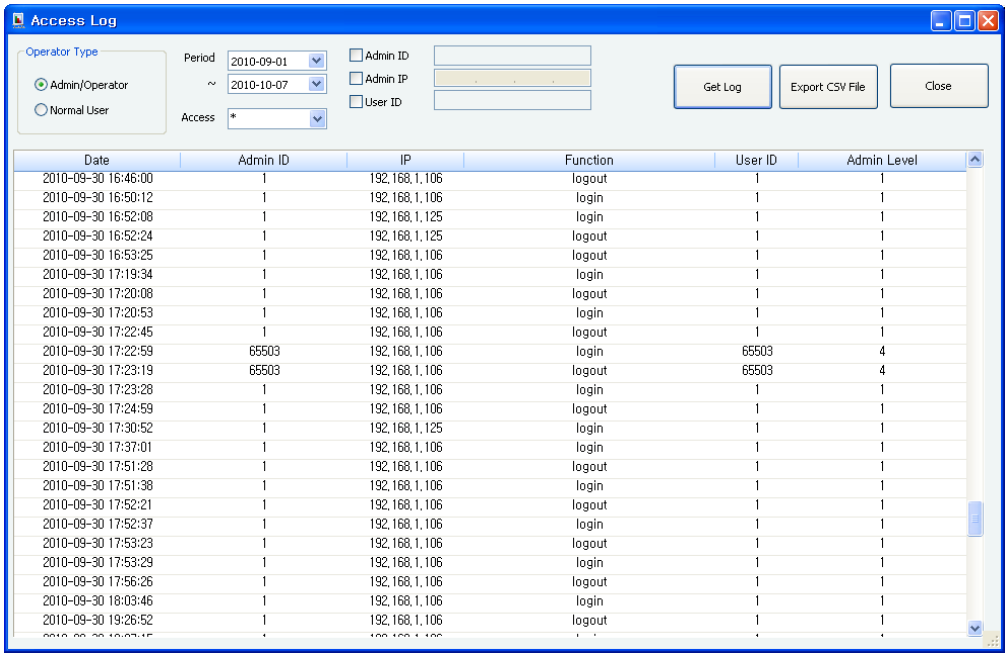
To view access logs:

1. From the menu bar, click **Administrator > Access Log**. This will open the **Access Log** dialog box.



2. Click a option button to select either administrators or users.
3. Set an event period (beginning and ending dates) with the drop-down calendars.
4. Select a type of access or modification event with the Access drop-down list.
5. If desired, specify a particular admin or user by clicking the checkbox next to the Admin ID, Admin IP, or User ID fields, and then entering the appropriate identification.

6. Click **Get Log**. This will generate a list of the relevant events for the period you specified.



4.3 Monitor Door Events via a Visual Map

BioStar allows you to conveniently manage doors on a visual representation of your actual floor plan. On the Visual Map, you can customize your floor plan, add doors, and monitor door status and activity (for example, whether the door is open or closed, authentication events, and door alarms). If you have more than one floor plan, you can create additional Visual Maps for each floor. The Visual Map feature is available only in the Standard Edition.

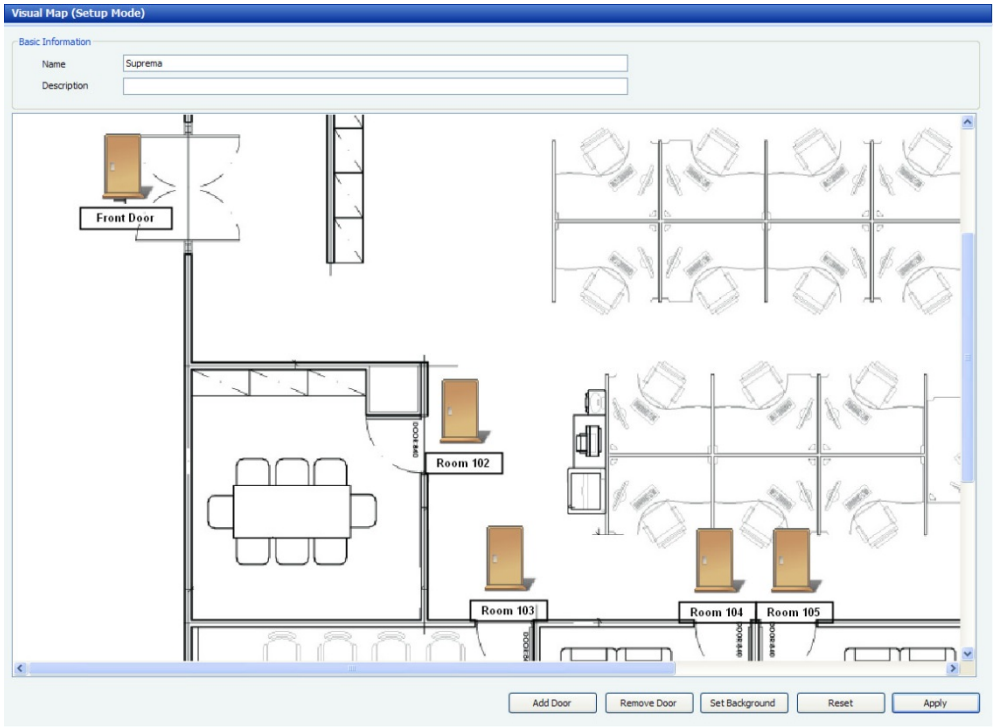
4.3.1 Create a Visual Map

In the setup mode, you can add the floor plan of your building and place doors.

To add the floor plan and place doors on the plan:

1. In the shortcut pane, click **Visual Map**.
2. In the task pane, click **Setup Mode**. “Monitor Mode” will appear in the title bar of the **Visual Map** window.
3. In the task pane, click **Add Visual Map**. This will open a new Visual Map window on the right.
4. In the Visual Map window, type a name for the new Visual Map.
5. At the bottom of the **Visual Map** window, click **Set Background** to add a floor plan. The BioStar supports images larger than resolution 730x470 in jpg, bmp, gif, or png format only.

6. Choose an image and click **Open**.
7. Click **Add Door** to add doors. This will open a window with a list of doors.
8. From the door list, click the checkboxes next to doors to add and click **Apply**. Door icons will appear on the floor plan.



9. Click and drag the door icon to the desired location on the floor plan. You can individually relocate a door icon or name by double-clicking the door icon or name.
10. To remove a door from the floor plan, click the door and then click **Remove Door**.
11. Repeat steps 7-10 as necessary to add additional doors.
12. When you are finished adding doors, click **Apply**.

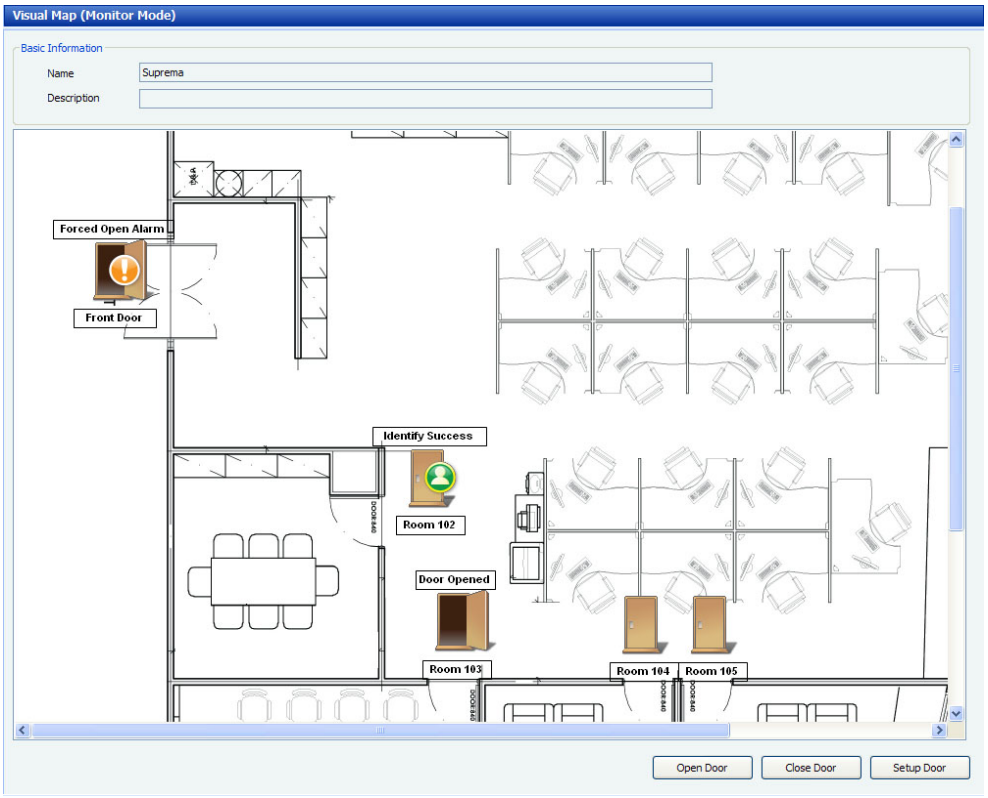
Note: To remove all doors from the plan and start over, click **Reset**.

4.3.2 Monitor Doors on a Visual Map

In the monitor mode, you can view the status and activities for each door on the visually enhanced map.

To monitor doors:

1. In the task pane, click **Monitor Visual Map**. “Monitor Mode” will appear in the title bar of the **Visual Map** window.



2. Monitor door status and activities on the visual map, as represented by the following icons. Door activities, such as successful authentication or alarms will appear on the door icons:

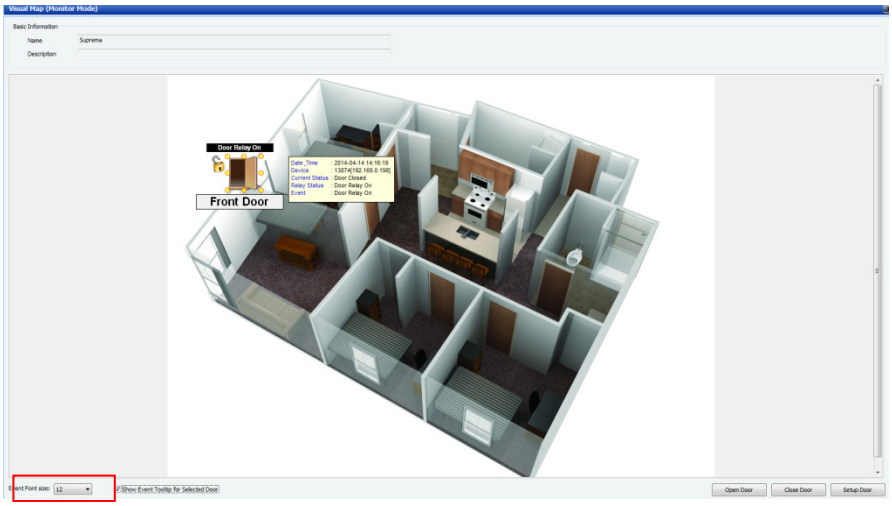
Icon	Activity
	Door is closed / Door alarm is clear
	Door is open
	Successful authentication while door is closed
	Successful authentication while door is open
	Failed authentication while door is closed
	Failed authentication while door is open
	Held or forced open door / Held or forced open door alarm

Note: Door icons will change only when door sensors have been assigned in the door settigns and detect the door status. In other words, door icons change only when the door

actually opens or closes and not when you click **Open Door** or **Close door.** For more information about door settings, see section 5.2.1.

3. To open or close a door, click a door and then click **Open Door** or **Close Door**. To change settings for a door, click a door and then click **Setup Door**.
4. The current relay status can be checked through Visual Map in Monitoring.

5. Show Event Tooltip for Selected Door option is added to indicate the details of the current door status.



6. Event or door name font size can be enlarged or reduced by selecting font size in Setup Visual Map and Monitor Visual.

4.4 Control Doors, Alarms, and Devices Remotely

BioStar allows administrators or operators to control doors, alarms, and devices remotely. You can open or close doors via a computer connected to the BioStar system. You can also release (cancel) alarms remotely and lock or unlock devices.

4.4.1 Open or Close Doors

In some situations, an administrator or operator may need to open or close a door remotely.

To open or close doors:

1. Click **Monitoring** in the shortcut pane.
2. The Door/Zone Monitoring tab lists door names and their statuses. To change the status (open or closed) of a door, click the door name and then click either **Open Door** or **Close Door**.

You can also open and close doors while monitoring a Visual Map. For more information, see section 4.3.2.

4.4.2 Release Alarms

When an event triggers an alarm, administrators or operators can release the alarm remotely.

To release alarms:

1. Click **Monitoring** in the shortcut pane.
2. The Door/Zone Monitoring tab lists doors names and alarm events. To release (cancel) an alarm, click the door name and then click **Release Alarm**.

4.4.3 Lock or Unlock Devices

BioStar allows you to lock and unlock devices to prevent unauthorized access when BioStar is not running. This action blocks communication from devices. You can either lock devices manually from the BioStar interface or automatically when you exit the BioStar software. All connected devices can be simultaneously locked or unlocked, but you cannot lock or unlock devices that are connected directly to the BioStar server.

4.4.3.1 Lock or unlock connected devices

To lock all connected devices, from the menu bar, click **Option > Device > Lock All Devices**.

To unlock all connected devices:

1. From the menu bar, click Option > Device > Unlock All Devices.
2. If necessary, enter a password in the **Enter Locking Password** dialog box and click **OK** (if you have not created a locking password, simply click **OK**). See section 4.4.3.2 to create a locking password.

Attention: 2.x devices (BioStation 2, BioStation A2, BioStation L2, BioEntry W2) do not support this function.

4.4.3.2 Set automatic device locking

To set automatic device locking:

1. From the menu bar, click **Option > Device > Automatic Locking**. This will open the **Auto Locking** dialog box.

2. Click the first checkbox to lock all devices when exiting BioStar.
3. If desired, click the second checkbox to change the lock password:
   a. Enter the old password
   b. Enter the new password
   c. Retype the new password to confirm.

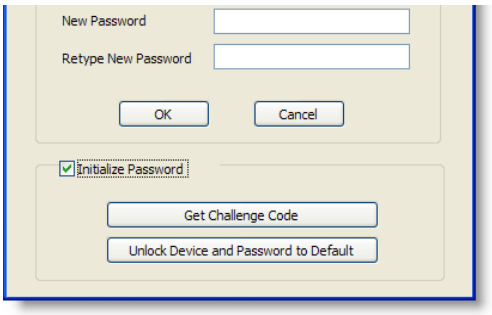
Attention: 2.x devices (BioStation 2, BioStation A2, BioStation L2, BioEntry W2) do not support this function.

4.4.3.3 Reset a device lock

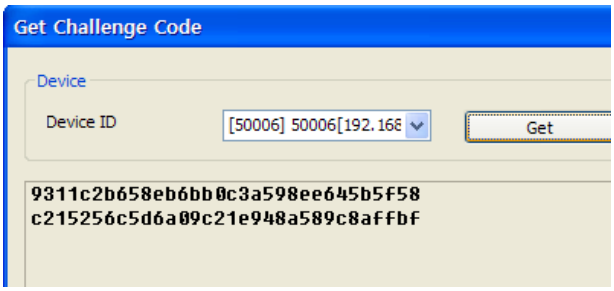
If you have forgotten the locking password for a device, Suprema's technical support team can send you an unlock code.

To request the code:

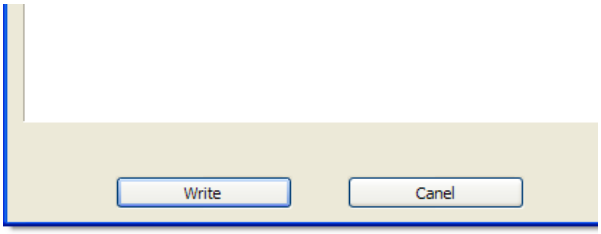
1. From the menu bar, click **Option > Device > Automatic Locking**. This will open the **Auto Locking** dialog box.



2. Click the Initialize Password checkbox to activate the buttons at the bottom of the screen.
3. Click **Get Challenge Code**. This will open the **Get Challenge Code** dialog box.



4. Select the appropriate device from the drop-down list and click **Get**.
5. Click **Save as File** to save the challenge code to your computer.
6. Email the challenge code to Suprema (*support@supremainc.com*). Suprema's technical support personnel will return an unlocking code to you via email.
7. When you receive the code from Suprema, open the **Auto Locking** dialog box and activate the buttons (see steps 1-2).
8. Click **Unlock Device and Password to Default**. This will open the **Write Challenge Code** dialog box.



9. Click **Open Code File** and locate the file sent to you by Suprema.

When you have opened the file, click **Write**. This will unlock the device and reset the locking password to the default (no password).

Attention: 2.x devices (BioStation 2, BioStation A2, BioStation L2, BioEntry W2) do not support this function.

4.5 Manage Users

With the BioStar system, you can delete users, transfer users to other departments, and customize user information fields. You can also export or import user data for creating custom reports, batch editing, or other needs.

4.5.1 Delete Users

If the occasion arises, you can easily remove users from the BioStar system.

To delete a user:

1. Click **User** in the shortcut pane.
2. Right-click a user's name.
3. Click *Delete User*.
4. Click **OK** to confirm the deletion.

4.5.1.1 Delete an individual user via command cards

After issuing command cards, you can delete an individual user directly from a BioEntry Plus, BioEntry W, or Xpass or Xpass S2 device. For more information about issuing command cards, please see section 3.2.6.1 and 3.2.8.1.

To delete users directly from a BioEntry Plus or BioEntry W device via command cards:

1. Place a delete card (command card) on a BioEntry Plus or BioEntry W device.
2. If authorization is required, an administrator must scan his or her fingerprints to continue.
3. Place the user's access card on the device and then have the user place his or her finger on the scanner (as prompted by the device).

To delete users directly from an Xpass or Xpass S2 device via command cards:

1. Place a delete card (command card) on an Xpass or Xpass S2 device.
2. If authorization is required, an administrator must place his or her access card on the device to continue.
3. Place the user's access card on the device.
4. Place the delete card on the device again to confirm the action.

4.5.1.2 Delete all users via command cards

After issuing command cards, you can delete all users directly from a BioEntry Plus, BioEntry W, or Xpass or Xpass S2 device. For more information about issuing command cards, see section 3.2.6.1 and 3.2.8.1.

To delete all users directly from a BioEntry Plus or BioEntry W device via command cards:

1. Place a delete all card (command card) on a BioEntry Plus or BioEntry W device.
2. If authorization is required, an administrator must scan his or her fingerprints to continue.
3. Place the delete all card on the device again to confirm the action.

To delete all users directly from an Xpass or Xpass S2 device via command cards:

1. Place a delete all card (command card) on an Xpass or Xpass S2 device.
2. If authorization is required, an administrator must place his or her access card on the device to continue.
3. Place the delete all card on the device again to confirm the action.

4.5.2 Transfer Users to Other Departments

BioStar makes moving users to other departments very simple. Before transferring a user, you must create a department.

To create a department:

1. Click **User** in the shortcut pane.
2. In the navigation pane, right-click *User* that is top level of department.
3. Click **Add Department**.
4. Enter a name for the department.

To transfer users to a department, simply click and drag a user name onto a department name.

Note: Up to four department levels can be created.

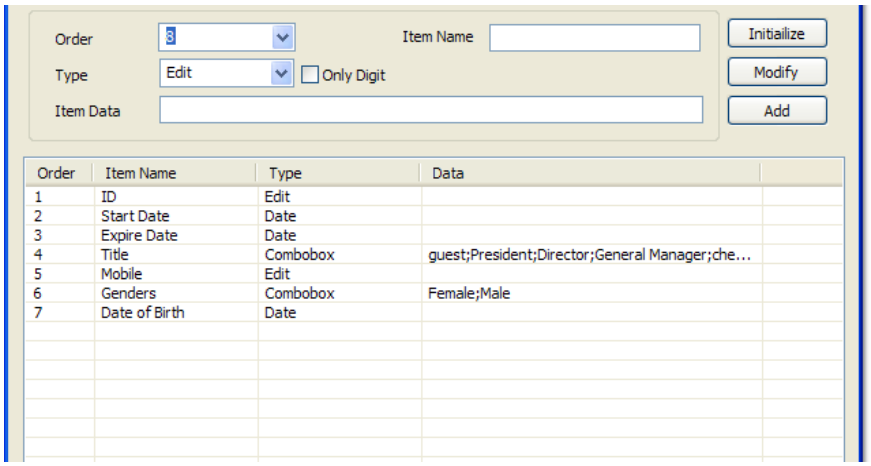
4.5.3 Customize User Information Fields

BioStar allows you to customize user information fields. This can be useful for altering the default information fields or for creating new fields.

4.5.3.1 Add new information fields

To add new information fields:

1. From the menu bar, click **Option > User > Custom Field Setting**. This will open the **Custom Fields Management** dialog box.



2. Select an order number from the first drop-down list (choose a number that is not already in use).
3. Select a field type from the second drop-down list. To restrict the field to numerical values, click the Only Digit checkbox.
4. Enter item data (for example, items to appear in a combo box) and a name for the item.
5. Click **Add**.
6. Repeat steps 2-5 as desired to create additional information fields.
7. When you are finished, click **Save**.

4.5.3.2 Modify existing information fields

To modify existing information fields:

1. From the menu bar, click **Option > User > Custom Field Setting**. This will open the **Custom Fields Management** dialog box (see section 4.5.3.1).
2. Click the item you want to modify in the list at the bottom. The data will appear in the fields at the top of the screen.

Note: Items 1-4 are required fields and cannot be modified or deleted.

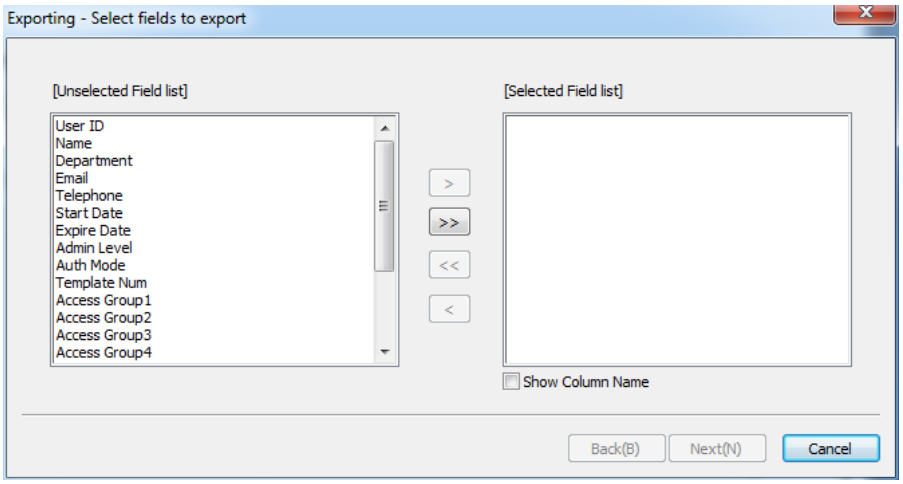
3. Modify the data as desired.
4. Click **Modify**.
5. Repeat steps 2-4 as desired to modify additional information fields.
6. When you are finished, click **Save**.

4.5.4 Export User Data

Exported user data is formatted as a comma-delimited file (CSV), which can be edited with a text editor or Microsoft Excel.

To export user data:

1. Click **User** in the shortcut pane.
2. In the task pane, click **Export User**. This will open the **Exporting** dialog box.



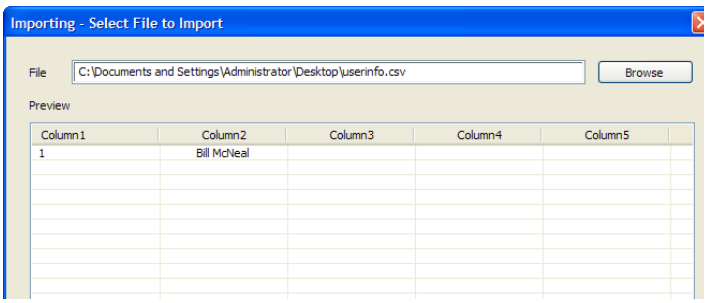
3. Select types of user data to export by clicking items in the list on the left and then clicking **>**.
4. Optional: Click **Show Column Name** below the selected filed list to include a field's column name with its data in an exported file.
5. After selecting all the types of user data to export, click **Next**.
6. Type a path and filename for the user data or click **Browse** to select a location to save the file.
7. Click **Next**.
8. Click **Export** to begin exporting the user data.
9. When the export is complete, click **Finish**.

4.5.5 Import User Data

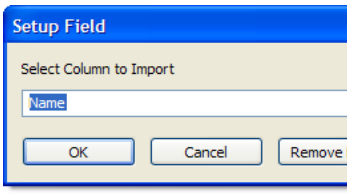
User data in comma-delimited format (CSV) can be imported to BioStar.

To import user data:

1. Click **User** in the shortcut pane.
2. In the task pane, click **Import User**. This will open the **Importing** dialog box.



3. Type a path and filename where the user data is located or click **Browse** to select a file.
4. Click **Next**. The raw data types will be displayed and the User list field will default to "Not Use. Click here to change."
5. Click the cell to the right of a data sample. This will open the **Setup Field** dialog box, which allows you to map the raw data to a user information field in BioStar.



6. Map the data to a field by selecting a field label from the drop-down list and then click **OK**.

Note: Up to four department levels can be displayed in BioStar. In the CSV file, include department levels in the same cell, separated by slashes (for example, "Department 1/Department 2/Department 3"), and then map the cell to the "Department" field in BioStar.

7. Repeat steps 5-6 as necessary to map additional data.
8. Click "Next" after matching data value and filed name correctly.

   If the CSV column type exported from BioStar has not been changed, you can drop 5-7 steps by the auto select button which enables to connect the column and field automatically.
9. Click **Import**.
10. If you map data to fields in an existing user account, you will prompted to confirm that you wish to overwrite the existing data. Click **Yes** or **Yes to All** to confirm or click **No** or **No to All** to deny.
11. Click **Finish**.

4.6 Manage Time and Attendance

BioStar allows you to monitor the time and attendance status of users and generate reports of T&A events, which you can edit or export as needed.

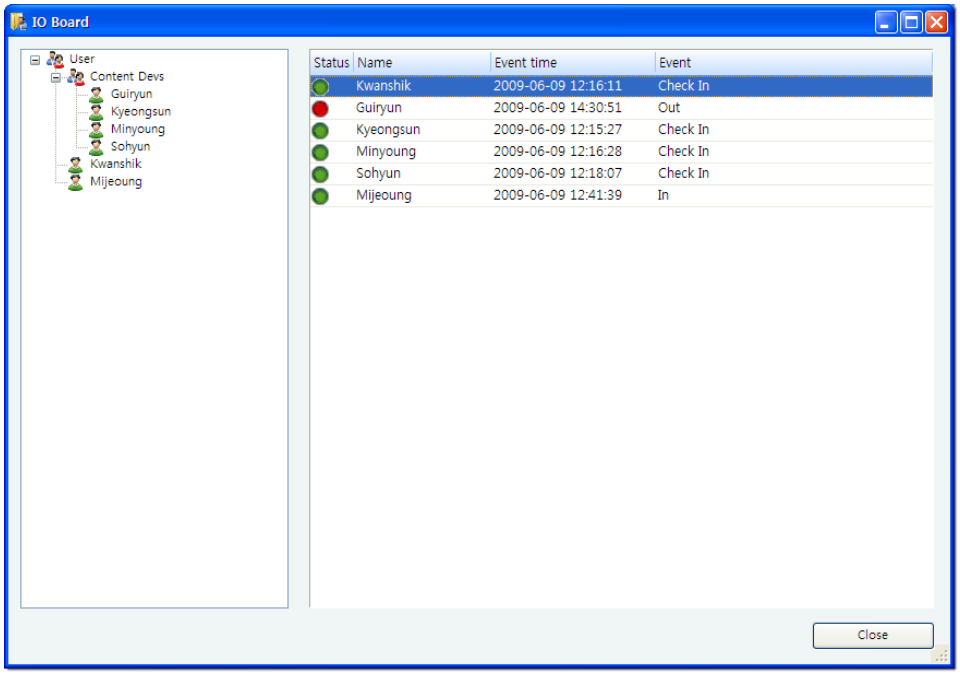
4.6.1 Monitor T&A Status via the IO Board

The IO Board displays time and attendance events only for entrance and exit events performed via the T&A function keys of access control devices. This feature is available only in the Standard Edition of BioStar.

You can use the board to verify recent T&A activities or to quickly determine which users are checked in or out. Users can use the board to view their own T&A activities.

To monitor the time and attendance status of users:

1. Click **Time and Attendance** in the shortcut pane.
2. From the task pane, click *IO Board*. This will open the **IO Board** dialog box.



3. Click **User**, a user name, or a department name in the pane on the left. This will display the corresponding T&A status in the pane on the right.
4. To close the dialog box, click **Close**.

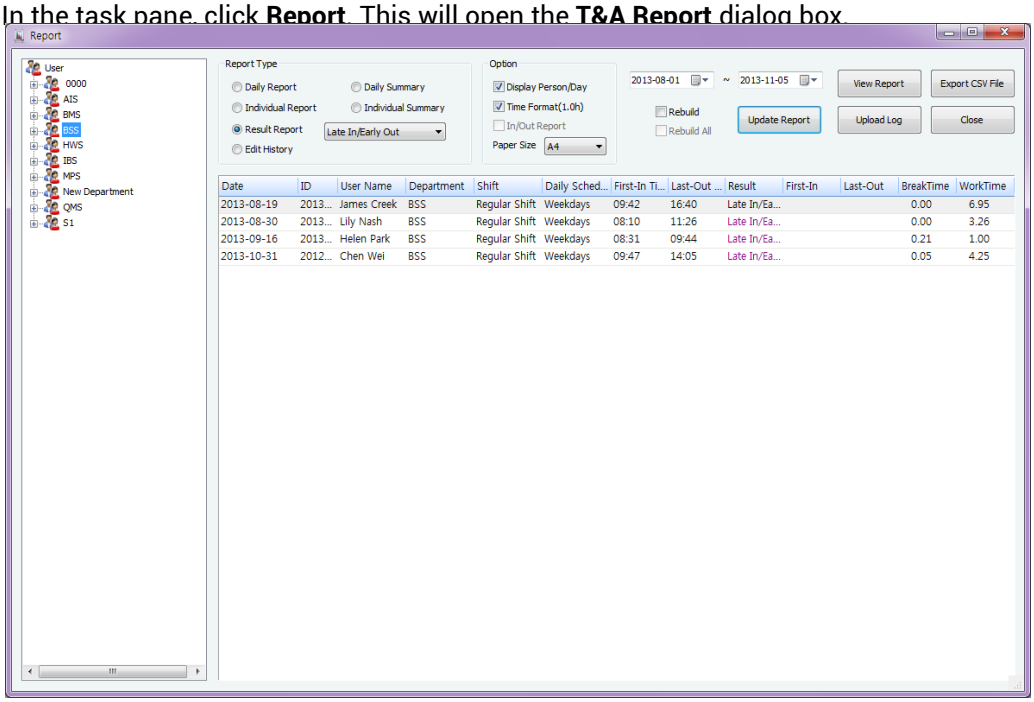
4.6.2 Generate T&A Reports

You can generate T&A reports to view various time and attendance events for users. You can also modify and print time and attendance data for other uses, such as calculating payrolls.

To generate a T&A report:

1. Click **Time and Attendance** in the shortcut pane.

2. In the task pane, click **Report**. This will open the **T&A Report** dialog box.



3. Click a option button to select a report type:
   - **Daily Report**: A report of all activities for the specified date range sorted by date.
   - **Individual Report**: A report of activities for the specified date range sorted by user ID.
   - **Result Report**: A report of activities that you specify via the drop-down list.
   - **Edit History**: A report of edited entries.
   - **Daily Summary:** A summary of activities for the specified date range sorted by date.
   - **Individual Summary**: A summary of activities for the specified date range sorted by user ID.

   Note: In case a simple hh: mm format is desired in your Daily Report and Individual Report rather than the original hh: mm(person) or hh: mm(day) style, click **Option > TA > Format** then click **Display person/day**.

4. Specify the detail options in the **Option** area.
   - **Display Person/Day**: Determine whether 'Person/Day' appears with data in the report.
   - **Time Format(1.0h)**: Display times in decimal dotted notation, for example, '1 Hr 7 Mins' is expressed in '1.11'.
   - **In/Out Report**: Display the times (up to the first 10 in and out times) when people are authenticated to enter and exit an office or a building.
   - **Paper Size**: Select A4 or Letter size paper.
5. Select a date range by clicking the drop-down calendars.
6. Click **View Report** to retrieve and display the results.

Note: Click **Upload Log** to retrieve data from all networked devices. Click **Update Report** to refresh the report with any data you have modified (see section 4.5.3).

You can sort report data by clicking any column header (the sort will toggle between ascending and descending orders). You can also rearrange the columns by dragging and dropping column headers in a new location. Furthermore, you can add or remove columns by using the menu that appears when you right-click on any column header:

To add a column to the report:

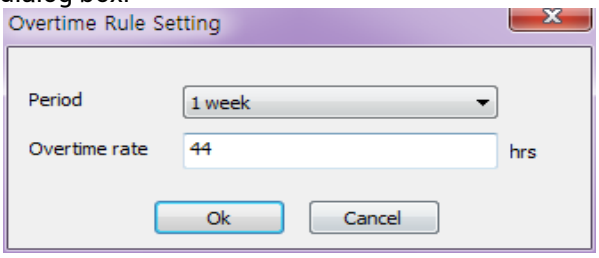
1. Right-**click** on any column header.
2. Click **Column** and select a column to add to the report.

To remove a column from the report:

1. Right-click on the column you want to remove.
2. Click **Remove column**.

To display overtime hours in the report:

1. Click Option > T&A > Overtime Rule Setting. This will open the Overtime Rule Setting dialog box.



2. Select a period unit which regular work hours are based on, and enter the amount of regular work corresponding to the period. The work hours that have exceeded the regular time would be considered overtime work and reported.
3. Click **OK**.

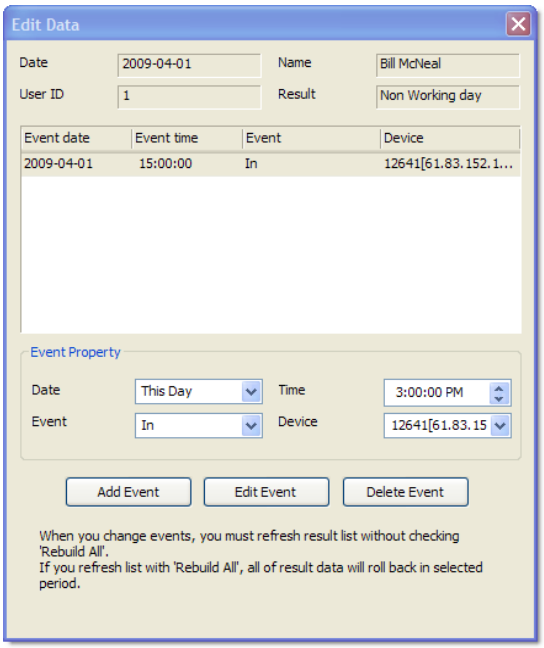
   Note: To successfully display overtime hours in a report, you should set the start day of the periold to Sunday of the week that you want to check for.

4.6.3 Modify T&A Reports

Time and attendance data can be modified for time reporting or payroll purposes. After generating a T&A report, you can locate cells that you want to modify and then click the cell and enter a new value or select an option from the drop-down list. This will save the modification to the report, but it will not overwrite the original data collected from access control devices. If you want to reproduce the report with the original data, click the checkbox next to "Rebuild" and then click **Update Report**.

To perform detailed modifications on report data:

1. Generate a T&A report as described in 4.5.2.
2. Right-click a cell and click **Detailed editing**. This will open the **Edit Data** dialog box.



3. To edit an event, change the following event properties as necessary and then click **Edit Event**. To add an event, change the following event properties as necessary and then click **Add Event**. To delete the event, click **Delete Event**.
   - **Date**: Select whether the event occurred on this day or the next day.
   - **Event**: Select the type of event.
   - **Time:** Set the time of the event.
   - **Device:** Set the device where the event occurred.
4. When you are finished modifying the event data, click the "X" in the top right corner to close the dialog box.
5. In the T&A Report window, ensure that the "Rebuild" checkbox is NOT checked.

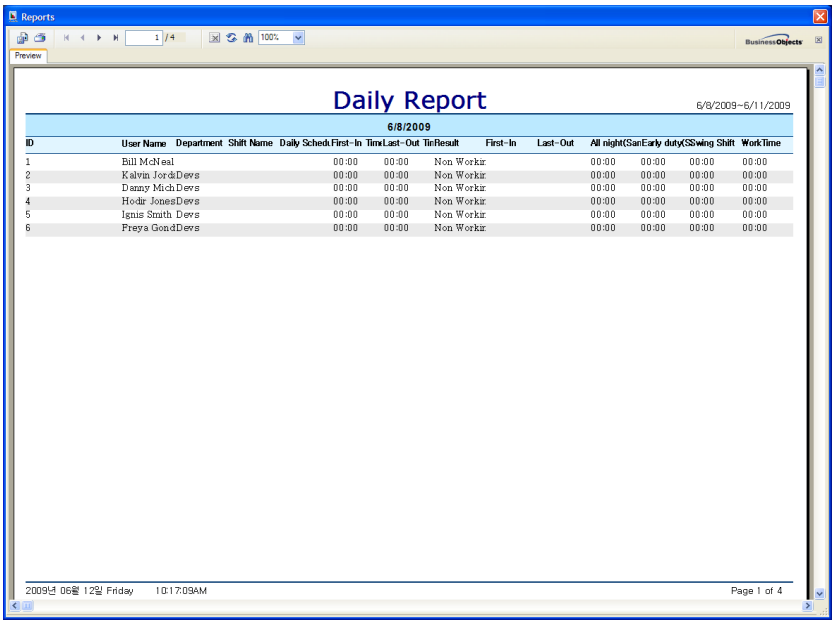
6. Click **Update Report**. The report will show the changes you have made. The changes you have made via the detailed editing will not be restored to the original data even if you click the check box next to “Rebuild” and click **Update Report**. If you want to reproduce the report with the original data, click the checkboxes next to “Rebuild” and “Rebuild All” and then click **Update Report**.

Note: You can sort report data by clicking any column header (the sort will toggle between ascending and descending orders). You can also rearrange the columns by dragging and dropping column headers in a new location.

4.6.4 Print or Export T&A Report Data

To print or export T&A report data:

1. Generate a T&A report as described in 4.5.2 and make any necessary modifications as described in 4.5.3.
2. Click **View Report**. This will open a preview window similar to the one below.



3. To print the report, click the print icon on the toolbar.
4. To export report data, click the export icon on the toolbar and then select an export format and a destination. You can export data in the following formats:
   - Adobe Acrobat (PDF)
   - Crystal Report (RPT)
   - HTML 3.2 or 4.0
   - Microsoft Excel 97-2000 or Microsoft Excel 97-2000–data only (XLS)
   - Microsoft Word or Microsoft Word–editable (RTF)
   - Open Database Connectivity (ODBC)
   - Record Style–Columns with spaces (REC)
   - Report Definition (TXT)

- Rich Text Format (RTF)
- Comma Separated Values (CSV)
- Tab Separated Text (TTX)
- Text (TXT)
- XML

Note: You can refresh the report data by clicking the refresh icon on the toolbar. You can also search for text in the report by clicking the search (binoculars) icon on the toolbar.

4.7 Manage Devices

You can easily remove devices, if necessary, and upgrade the device firmware directly from the BioStar interface. When removing devices, first ensure that any new data that may have been added at the terminal has been transferred to the BioStar server.

4.7.1 Remove Devices

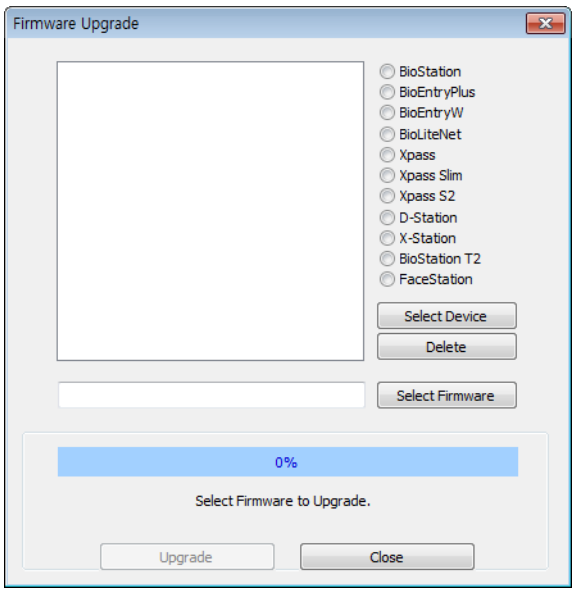
If you need to remove a device from the BioStar system, click **Device** in the shortcut pane, then right-click the device name and click *Remove Device*.

4.7.2 Upgrade Device Firmware

On occasion, it is necessary to upgrade your devices to the latest firmware version.

To upgrade device firmware:

1. From the menu bar, click **Option > Device > Firmware Upgrade**. This will open the **Firmware Upgrade** dialog box.



2. Click the option button next to the type of device you want to upgrade.
3. Click **Select Device** and select a device or devices from the **Device Tree** dialog box.

4. Click **OK** to close the **Device Tree** dialog box.
5. Click **Select Firmware**.
6. Locate the firmware file on your computer or network and click **Open**.
7. Click **Upgrade**.
8. When the firmware upgrade is complete, wait for the device to restart, and then click **Close**.

4.7.3 Downgrade Device Firmware

Devices may not work properly if downgraded or reverted back to an older version of firmware. Suprema does not recommend a downgrade. If your devices require a downgrade, please contact Suprema Technical Support (Email: support@supremainc.com), your Suprema distributor, or a local Suprema dealer.

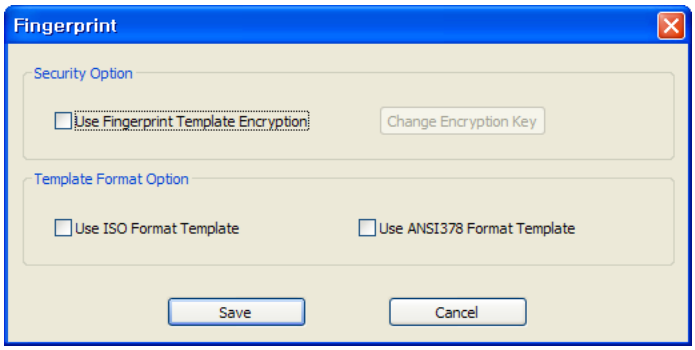
4.8 Activate Fingerprint Encryption

By default, additional fingerprint encryption is turned off. In most cases, activating this encryption is unnecessary. However, you may choose to turn on the encryption to provide extra security or privacy. Keep in mind that activating fingerprint encryption requires management of encryption keys and should be performed only by advanced users.

Activating fingerprint encryption will render all previously saved templates unusable. As a result, it is best to activate the encryption prior to registering users.

To activate fingerprint encryption:

1. From the menu bar, click **Option > Fingerprint**. This will open the **Fingerprint** dialog box.



2. Click the checkbox under “Security Option” to activate the fingerprint template encryption.

3. Click **Yes** to acknowledge the warning statement.
4. If desired, you may also change the encryption key:
   a. Click **Encryption Key**. This will open the **Change Encryption Key** dialog box.

   b. Enter a new encryption key in the first field.
   c. Confirm the key by entering it in the second field.
   d. Click **Change**.
5. Click **Save**. The option you have chosen will appear on the Fingerprint tab in the Device pane.

4.9 Change the Fingerprint Template

BioStar offers three types of fingerprint templates: ISO 19794-2, ANSI378, or Suprema's proprietary format. Suprema's format is active by default. Changing fingerprint template options will render all previously saved templates unusable. As a result, it is best to choose a template option prior to registering users.

Attention: The user's fingerprint format change and encryption should be set before the user's fingerprint is registered. If the fingerprint format changes and encryption is carried out after the fingerprint is registered, it should be carried out after all user settings screens are closed. In addition, if it is changed while the user settings screens are being selected, use BioStar Client after restarting it.

To change the fingerprint template option:

1. From the menu bar, click **Option > Fingerprint**. This will open the **Fingerprint** dialog box.
2. Click the checkbox under “Use ISO Format Template” to select the ISO format or “Use ANSI378 Format Template” to select the ANSI format.
3. Click **Yes** to acknowledge the warning statement.
4. Click **Save**.

05 Customize Settings

This section describes the settings available in the BioStar software. BioStar provides precise control and customization of the access control system via settings for device functions, door and zone behaviors, and user accounts.

5.1 Customize Device Settings

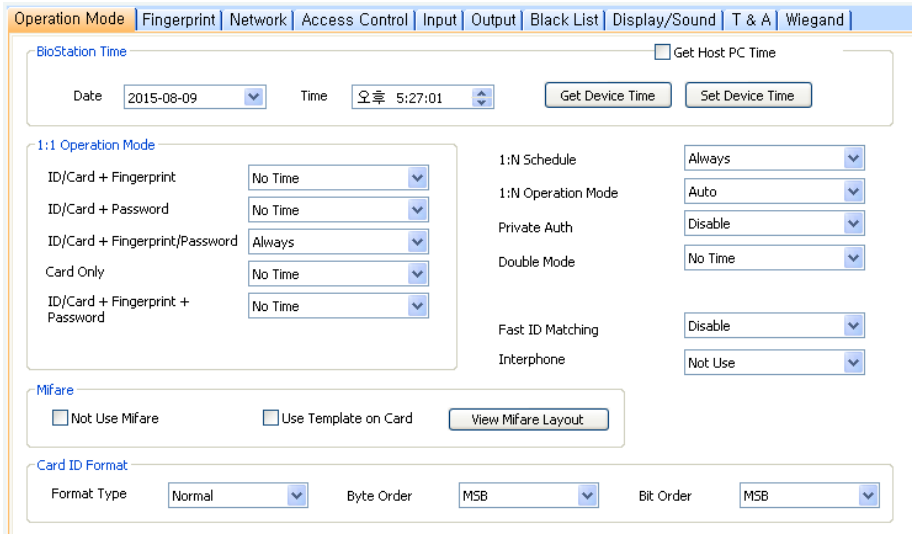
While most device settings are similar for BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2 and X-Station devices, the devices provide slightly different capabilities. BioStation 2, BioStation A2, BioStation L2 and BioEntry W2 support BioStar 2 by default and setting may be different from BioStar 2. The sections that follow describe the settings for each device separately. To access the tabs described below, click **Device** in the shortcut pane, then click a device name.

5.1.1 Customize Settings for BioStation Devices

The sections that follow describe the settings available for BioStation devices. Customize the way BioStation devices function by changing these settings to suit your particular environment and operational needs.

5.1.1.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation devices.



- **BioStation Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time:** Manually set the device time.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **1: 1 Operation Mode**: the drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID/Card + Fingerprint:** Set the device to require ID or card plus fingerprint authorization (*Always*, *Disable*, or custom schedule).
  - **ID/Card + Password:** Set the device to require ID or card plus password authorization (*Always*, *Disable*, or custom schedule).
  - **ID/Card + Fingerprint/Password:** Set the device to require ID or card plus fingerprint or password authorization (*Always*, *Disable*, or custom schedule).
  - **Card Only**: Set the device to require only card authorization (*Always*, *Disable*, or custom schedule).

  - **ID/Card + Fingerprint + Password:** Set the device to require ID or card plus fingerprint plus password authorization (*Always*, *Disable*, or custom schedule).

- **Mifare** (available only on BioStation Mifare devices)
  - **Not Use Mifare**: Check this box to disable MIFARE card authorization.
  - **Use Template on Card:** Check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order:** Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).
- **Other Options**
  - **1: N Schedule**: Set a schedule for using fingerprint only authentication (*Always*, *Disable*, or custom schedule).
  - **1: N Operation Mode:** Set a method for activating the fingerprint sensor (*Auto*, *Ok/Function Key*, or *None*).
  - **Private Auth**: Set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
  - **Double Mode:** Set the device to require authentication of two users' access cards or fingerprints (*Always*, *Disable*, or custom schedule). The timeout for presenting the second authentication is 15 seconds.
  - **Fast ID Matching:** Set the device to allow quicker authentication, by requiring users to input only the first two digits of the user ID and scan a single fingerprint (Enable or Disable). This option attempts authentication for a smaller subset of users (only those with the same first two digits in their user IDs) to increase matching speed.

    Note: This option does not support server matching (see 5.1.1.2). When using function keys for T&A events (see 5.1.1.8), only keys F1-F4 are supported (BioStation V1.7 and higher).
  - **Interphone:** Set the device to act as an interphone to allow communication between people on either side of the door (*Not Use* or *Use*).

In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.

Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3,
BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

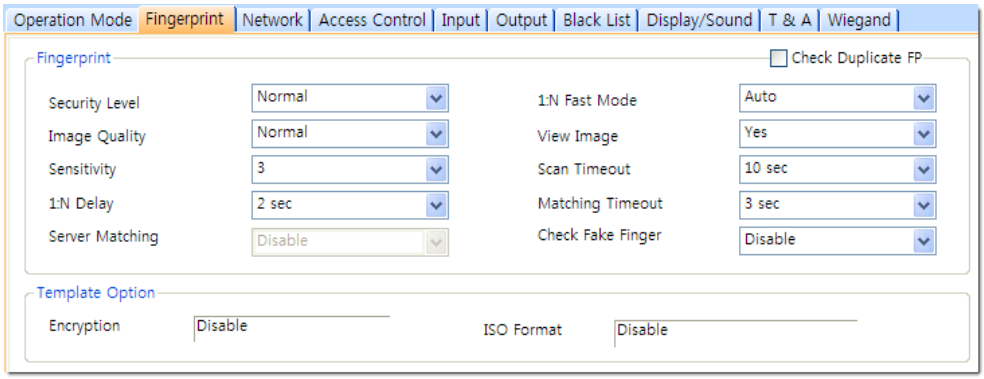
- Use Wiegand Card Bypass: By Wiegand setting in BioStar, this feature exports CSN regardless of whether the authentication is successful or not. This is designed to be used as a dummy reader that doesn't have a door control feature. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

  Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3,
  BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

  –

5.1.1.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation devices.



- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Image Quality**: Set the strictness of the quality check for fingerprint scans (*Weak*, *Normal*, or *Strict*). If a fingerprint image is below the specified quality level, it will be rejected.
  - **Sensitivity**: Set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **1: N Delay:** Set the delay between scans when identifying fingerprints (*0 sec* to *10 sec*). This delay prevents the scanner from processing

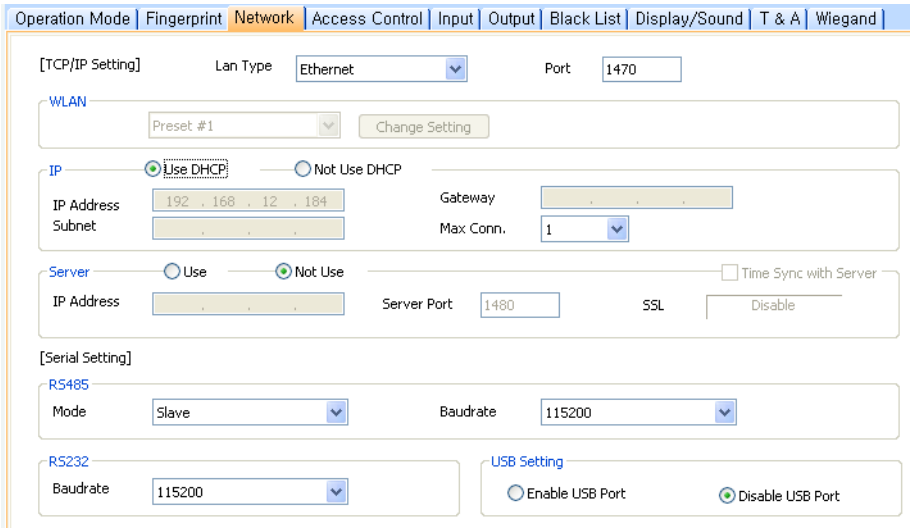
the same fingerprint more than once if a user has not yet removed his or her finger from the scanner.

- **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
- **View Image**: Set to show or hide fingerprint images on the BioStation display (*Yes* or *No*).
- **Scan Timeout**: Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
- **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
- **Server Matching**: Enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.

- **Check Duplicate FP**: Set the device to determine whether or not a scanned fingerprint has been previously enrolled. If the device determines that a fingerprint has been previously enrolled, the enrollment process will fail.

5.1.1.3 Network tab

The Network tab allows you to customize network and server settings for BioStation devices.

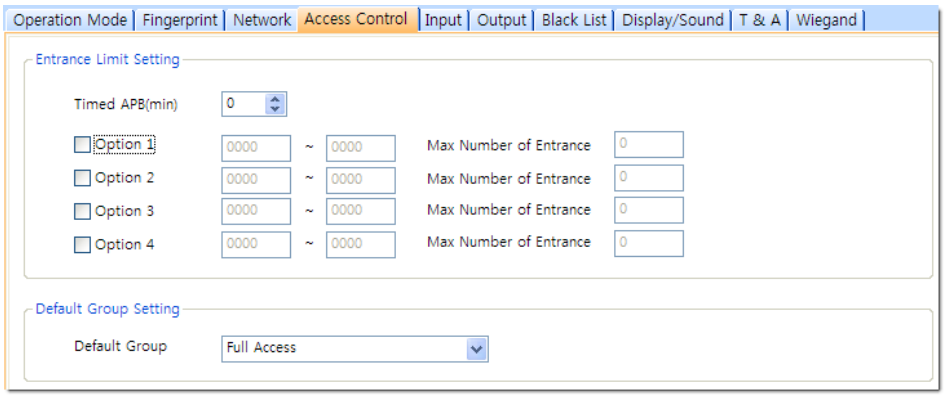


- **TCP/IP Setting**

  - **LAN Type:** Select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port**: Specify a port to use for the device.
  - **WLAN:** Select a preset WLAN configuration from the drop-down list. This option is active only when WLAN is selected as the TCP/IP setting.
  - **Change Setting**: Click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, please see section 3.2.4.
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet:** Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Max Conn.**: Specify the maximum number of connections to allow.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button to disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port:** Specify the port used to connect to the server.
  - **SSL**: Displays the status of SSL for the server connection.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **RS485**
  - **Mode:** Set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232**: Set the baud rate for a device connected via RS232 (*9600* to *115200*).
- **USB Setting**: Click the option buttons to enable or disable the USB port on the BioStation device.

5.1.1.4 Access Control tab

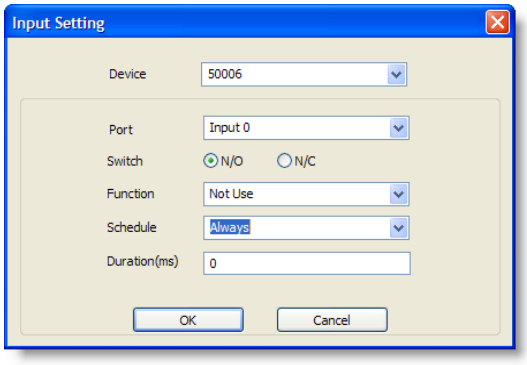
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioStation device.



- **Entrance Limit Setting**
  - **Timed APB (min):** Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance:** Set the maximum number of entries allowed during the specified time limit.
- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.1.5 Input tab

The input tab lists input settings you have specified for a BioStation device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.

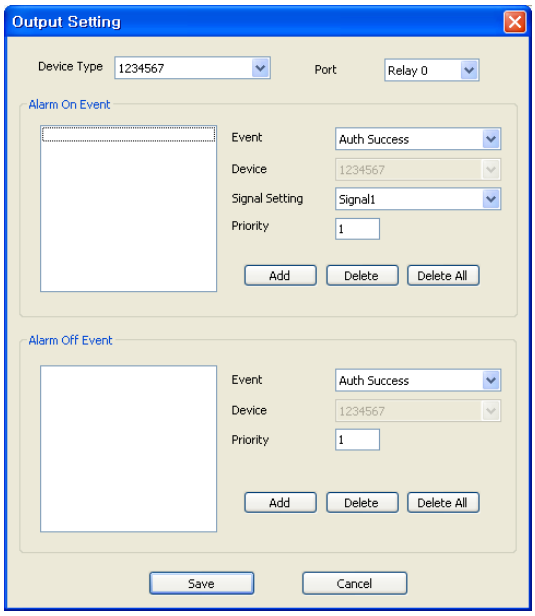


- **Device**: Select the BioStation (or Secure I/O) device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).

- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input:** The input port will be monitored for a triggering action (For the events specified with “Detect Input 0-3” in the **Output Setting** dialog box, please see section 5.1.1.6).
  - **Emergency Open:** Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms***:* Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device:** Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.
  - With BioStar 1.8v, LED Green Input, LED Red Input, Buzzer Input, Access Granted Input, and Access Denied Input were newly added. And these input options are available only with BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), and Xpass (FW 1.3v).
- **Schedule:** Set the schedule during which the inputs will be monitored (*Always*, *Disable*, or custom schedule).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.1.6 Output tab

The Output tab lists output settings you have specified for a BioStation device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, please see section 3.10.3.1.

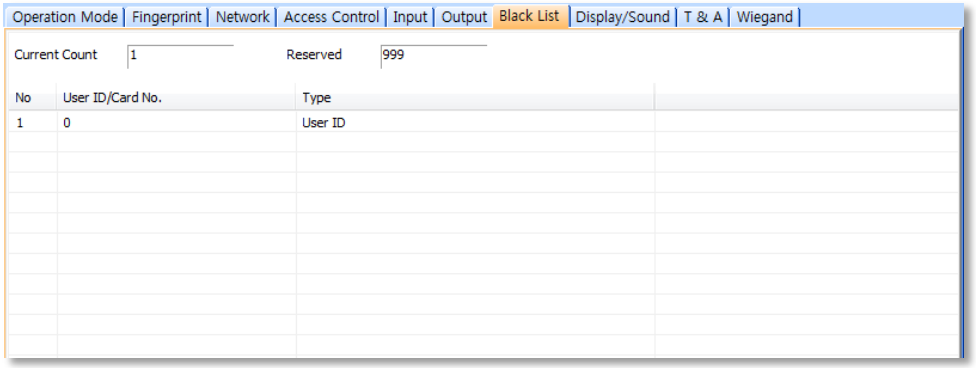


- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: Select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event:** Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Signal Setting:** Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority:** set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For

example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.1.7 Black List tab

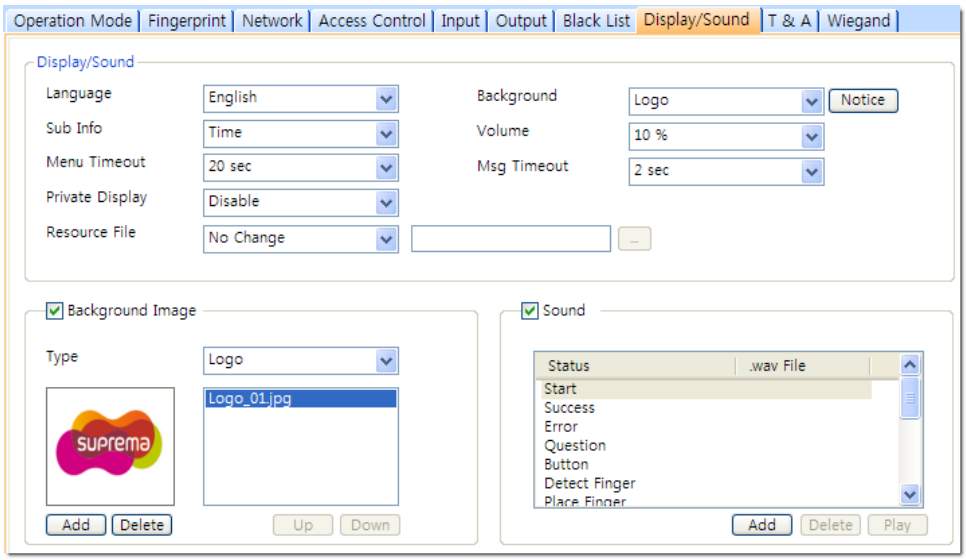
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of user IDs and access cards that have been registered.
- **Reserved**: The remaining number of user IDs and access cards that can be registered.

5.1.1.8 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



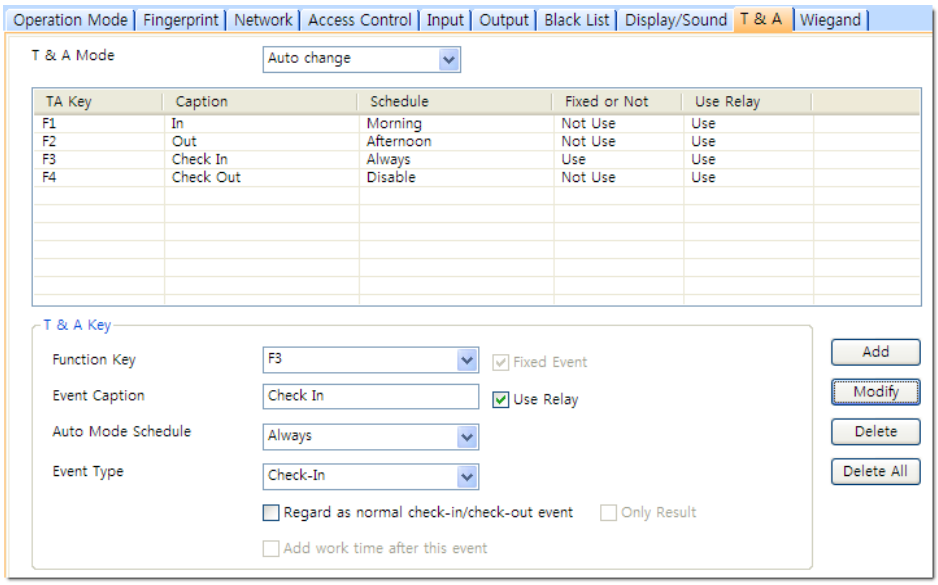
- **Display/Sound**
  - **Language**: Set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Sub Info**: Set the info to display at the bottom of the BioStation display (*Time*, or *None*).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen (*Infinite*, *10 sec*, *20 sec*, or *30 sec*).
  - **Private Msg**: Enable or disable the option to show a private message on the BioStation display (*Disable* or *Enable*). You can add a private message from the Event tab in the User pane: click **Modify Private Information**, set options for display count and display duration, enter text in the Private Message field, and then click **Save**.
  - **Resource**: Set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the BioStation display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 320x240 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
  - **Notice**: Click this button to create a notice that will be shown on the BioStation display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.

  - **Volume**: Set the volume of the BioStation device (*10%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed.

- **Background Image**: Click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.
- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file.

5.1.1.9 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



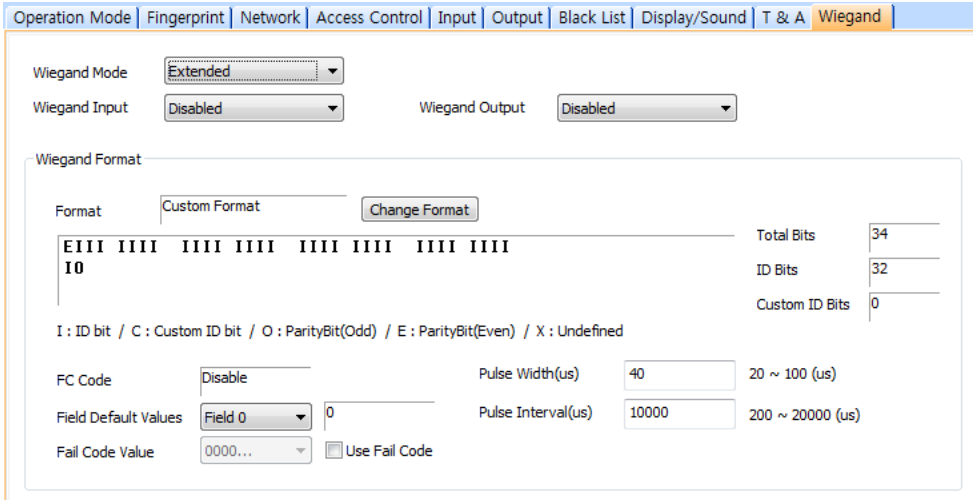
- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key:** Select a function key from the drop-down list to assign a T&A event (*F1-F4*, *1-9*, *CALL*, *0*, or *ESC*). If you are using the Event

Fix mode, you can click the checkbox to the right to designate a fixed event.

- **Event Caption:** Enter a caption for the event.
- **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
- **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.1.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.16.



- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card

readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.

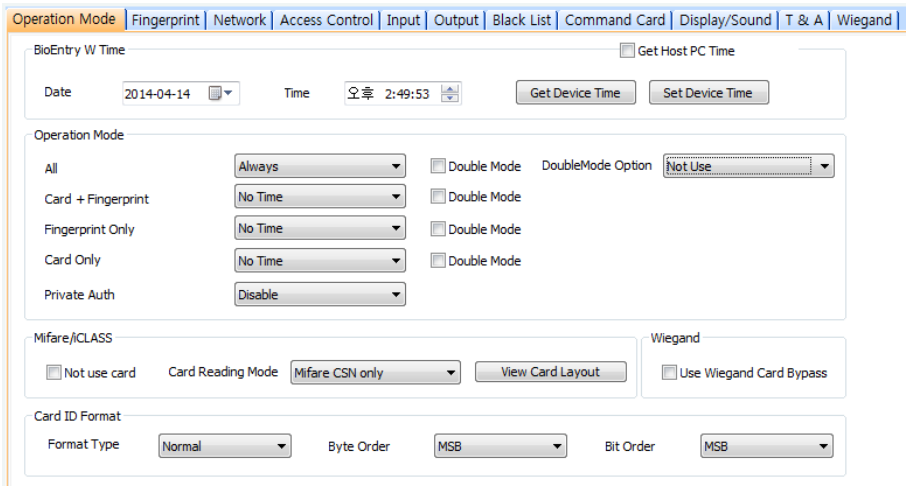
- **Wiegand Input**: Assign the Wiegand input:
  - **Disabled**: The input will not be used.
  - **Wiegand [Card]**: The ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]**: The ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output**: Assign the Wiegand output:
  - **Disabled**: The output will not be used.
  - **Wiegand [Card]**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.2 Customize Settings for BioEntry Plus or BioEntry W Devices

The sections below describe the settings available for BioEntry Plus and BioEntry W devices. Customize the way BioEntry Plus or BioEntry W devices function by changing these settings to suit your particular environment and operational needs.

5.1.2.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioEntry Plus or BioEntry W devices.



- **BioEntry Plus Time/BioEntry W Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time**: Manually set the device time.

In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not

activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.

Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

- Use Wiegand Card Bypass: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

  Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.)

  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.

- **Operation Mode**: For each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.
  - **All**: Set the device to allow all types of authorization (*Always*, *Disable*, or custom schedule).
  - **Card + Fingerprint**: Set the device to require card plus fingerprint authorization (*Always*, *Disable*, or custom schedule).
  - **Only Fingerprint:** Set the device to require only fingerprint authorization (*Always*, *Disable*, or custom schedule).
  - **Only CARD**: Set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
  - **Private Auth**: Set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's authorization setting (Private Auth Mode), which is located on the Details tab in the User pane. If disabled, the authentication mode will be determined by the operation mode settings of the device.
  - **Double Verification Mode**: Set the device to require verification from two users during a selected schedule (*Always*, *Disable*, or custom schedule).

- **Mifare/iCLASS (available on select models)**
  - **Bio Entry Plus Mifare devices:**
  - **Not Use Card**: Check this box to disable MIFARE card authorization.

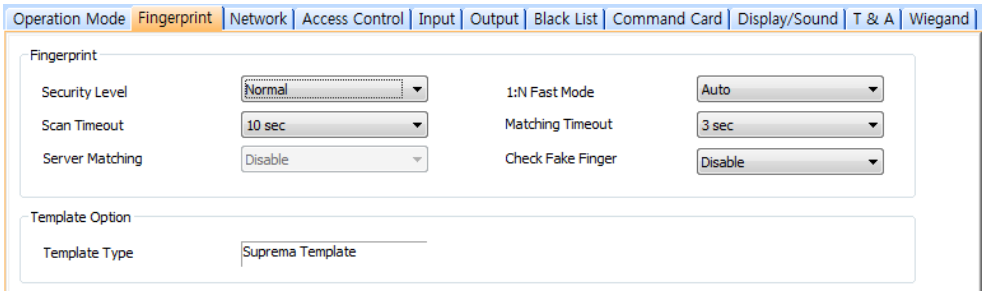
  - **Card Reading Mode**: Set the type of card authorization mode (*Mifare Template* or *Mifare CSN only*)
  - **View Mifare Layout:** Click this button to configure the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.

- **Bio Entry Plus iCLASS devices:**
  - **Not Use Card**: Check this box to disable iCLASS or FeliCa card authorization.
  - **Card Reading Mode**: Set the type of card authorization mode (*iCLASS Template*, *iCLASS CSN only*, or *FeliCa CSN only*).
  - **View Card Layout:** Click this button to configure the iCLASS layout used by the device. For more information about configuring iCLASS layouts, please see section 3.6.4.7.

- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order:** Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.2.2 Fingerprint tab

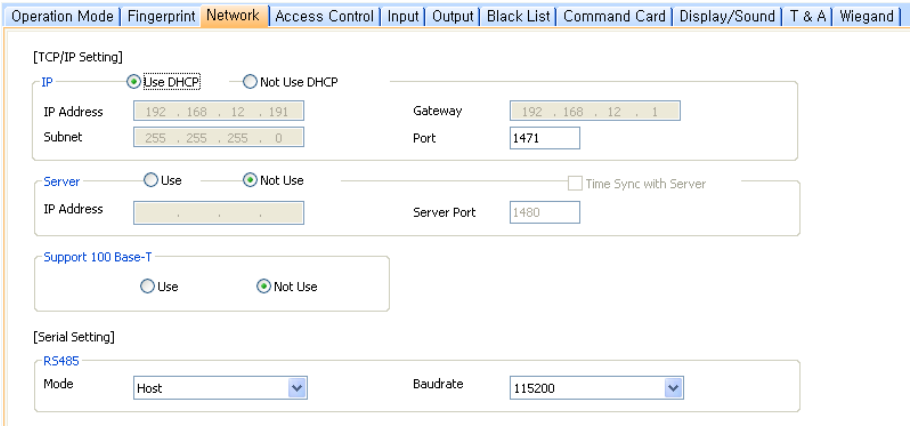
The Fingerprint tab allows you to customize fingerprint authorization settings for BioEntry Plus or BioEntry W devices.



- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Scan Timeout:** Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Server Matching**: Enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
  - **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.

5.1.2.3 Network tab

The Network tab allows you to customize network and server settings for BioEntry Plus or BioEntry W devices.

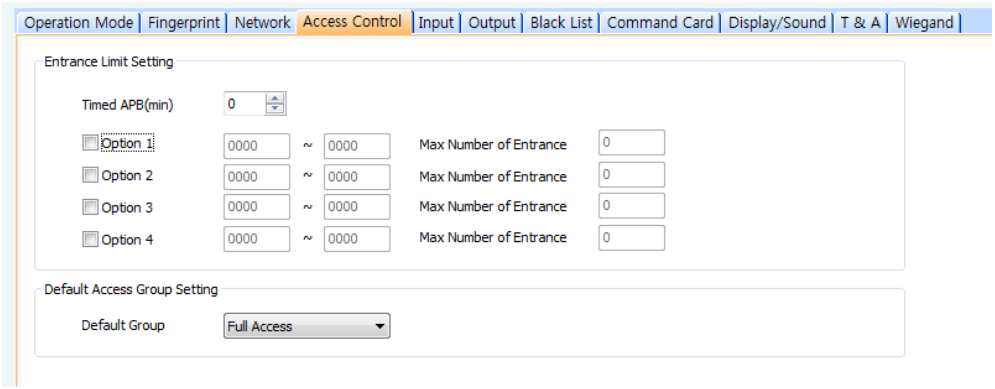


- **TCP/IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet**: Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Port:** Specify a port to use for the device.
- **Server**
  - **Use**: Click this option button to use specific server settings.
  - **Not Use**: Click this option button to disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **Support 100 Base-T:** This option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.
  - **Use**: Click this option button to enable the 100base-T connection for the device.
  - **Not Use**: Click this option button to disable the 100base-T connection for the device.
- **RS485**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).
- Support MTU Size setting

– Devices affiliated with Black Fin support MTU Size setting. The supported packet size is between 1078 and 1514, and the default is 1514.
Note: This feature is supported from the FW versions, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

5.1.2.4 Access Control tab

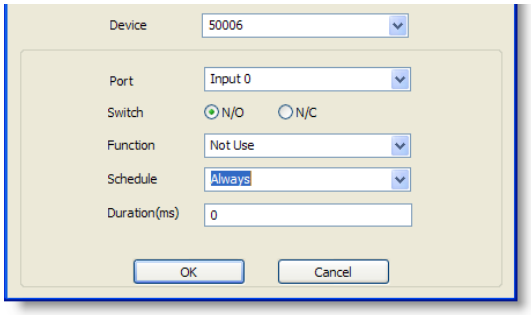
The Access Control tab allows you to customize entrance limit settings and default access groups, and T&A mode settings for a BioEntry Plus or BioEntry W device.



- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance:** Set the maximum number of entries allowed during the specified time limit.
- **Default Access Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.
- Automatic T&A Mode Change
  - **T&A Mode**: Set the time and attendance mode for the device (*Disable*, *Fixed In*, *Fixed Out*, and *Auto*).
  - **Fixed Entrance:** When the "Auto" T&A mode is selected, specify when to allow entrance events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
  - **Fixed Exit Time:** When the "Auto" T&A mode is selected, specify when to allow exit events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
  - **In Event Caption**: Set a caption for check-in.
  - **Out Event Caption**: Set a caption for check-out.

5.1.2.5 Input tab

The input tab lists input settings you have specified for a BioEntry Plus or BioEntry W device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.



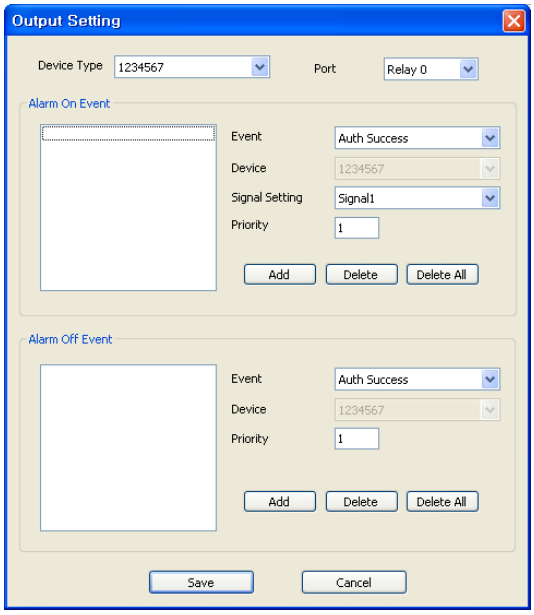
- **Device**: Select the BioEntry Plus or BioEntry W (or Secure I/O) device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch:** Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input:** The input port will be monitored for a triggering action (events specified with "Detect Input 1-3" in the **Output setting** dialog box —see section 5.1.2.6).
  - **Emergency Open**: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device:** Restart the device.
  - **Disable Device:** Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.

– With BioStar 1.8v, LED Green Input, LED Red Input, Buzzer Input, Access Granted Input, and Access Denied Input were newly added. And these input options are available only with BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), and Xpass (FW 1.3v).

- **Schedule**: Set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.2.6 Output tab

The Output tab lists output settings you have specified for a BioEntry Plus or BioEntry W device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.



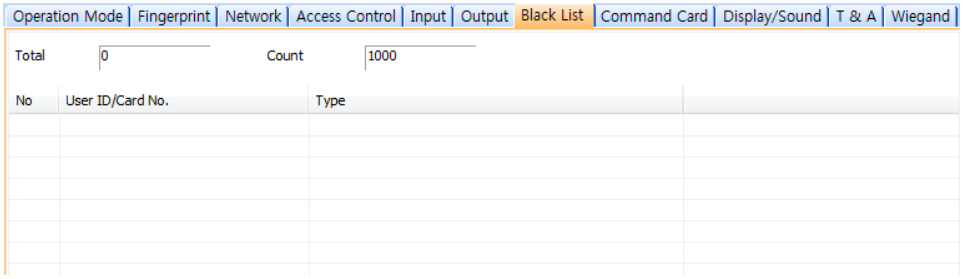
- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: Select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device:** Select the device to monitor for an alarm event.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be

canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.2.7 Black List tab

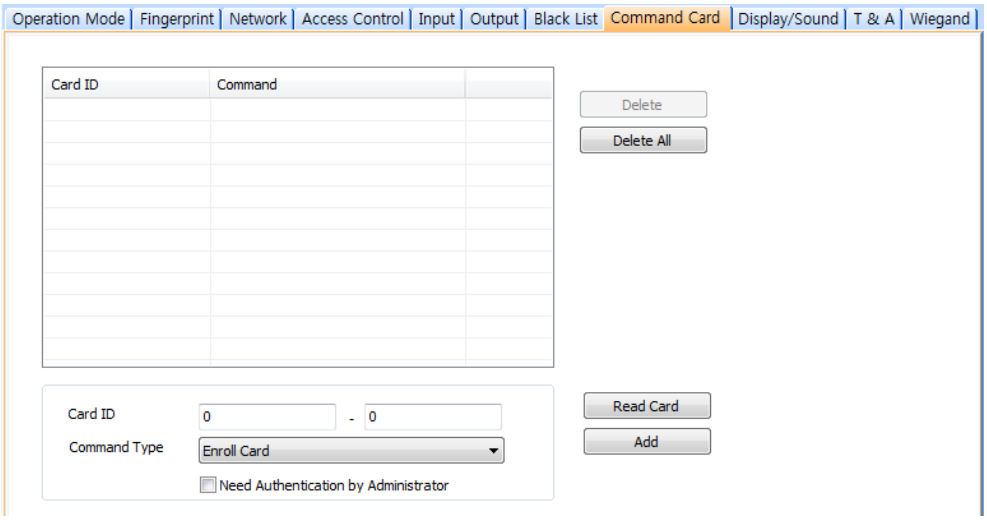
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of user IDs and access cards that have been registered.
- **Reserved**: The remaining number of user IDs and access cards that can be registered.

5.1.2.8 Command Card tab

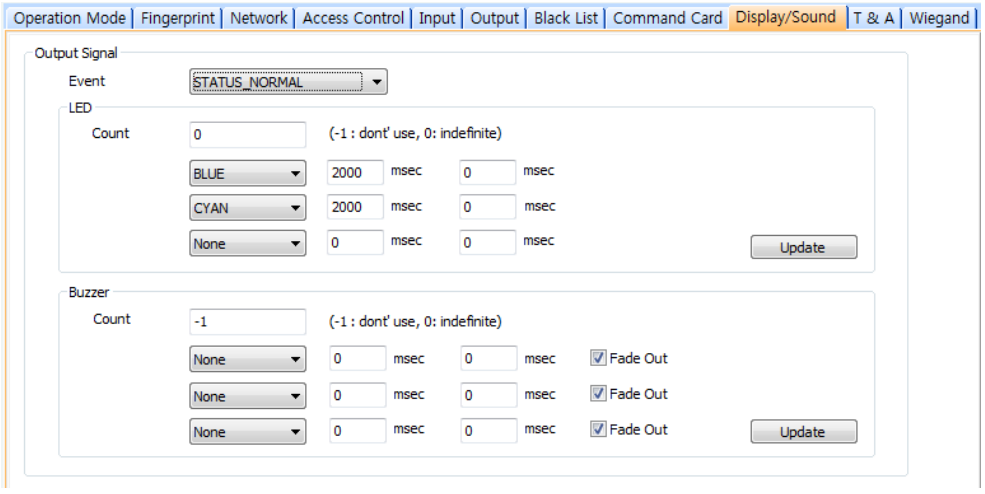
The Command Card tab allows you to issue command cards. For more information about command cards, see section 3.2.6.1.



- **Card ID**: Enter the card ID or click **Read Card** and place a command card on the reader to automatically populate the fields.
- **Command Type**: Select a type of command card to issue (*Enroll Card*, *Delete Card*, or *Delete All Card*).

5.1.2.9 Display/Sound tab

The Display/Sound tab allows you to customize the LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



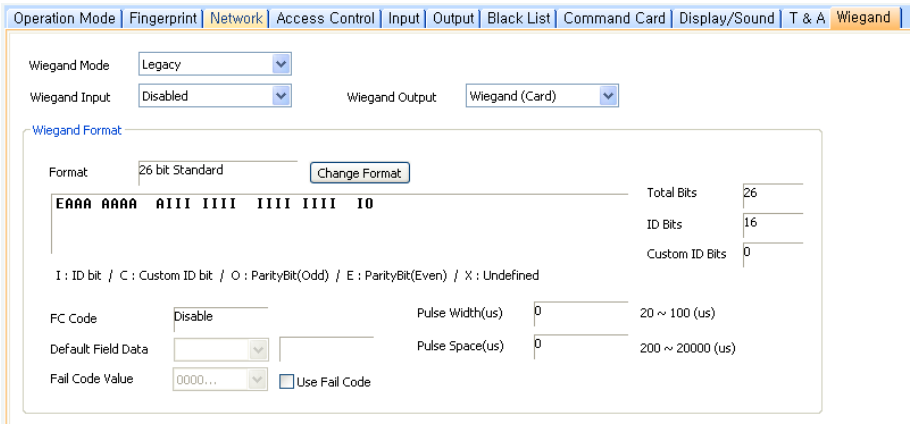
- **Event**: Specify the affected event by selecting it from the drop-down list.
- **LED**: Set the LED behavior for a specified event.
  - **Count**: Enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.

  - **Colors**: Specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.

- **Buzzer**: Set the buzzer behavior for a specified event.
  - **Count**: Enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume**: Set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out**: Set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.2.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioEntry Plus or BioEntry W device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for a BioEntry Plus or BioEntry W device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.16.



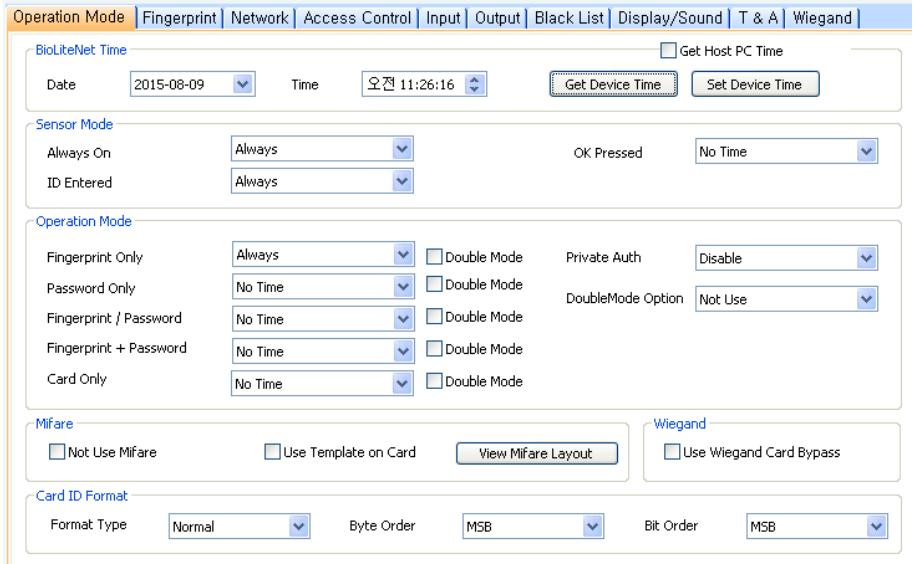
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input**: Assign the Wiegand input:
  - **Disabled**: The input will not be used.
  - **Wiegand [Card]**: The ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]**: The ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output**: Assign the Wiegand output:
  - **Disabled**: The output will not be used.
  - **Wiegand [Card]**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.3 Customize Settings for BioLite Net Devices

The sections that follow describe the settings available for BioLite Net devices. Customize the way BioLite Net devices function by changing these settings to suit your particular environment and operational needs.

5.1.3.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioLite Net devices.



- **BioLiteNet Time**

  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time:** Manually set the device time.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time:** Set the time on the device.

- **Sensor Mode**
  - **Always On**: Set the device sensor to be always available on standby (*Always* or *Disable*).
  - **ID Entered:** Set the device sensor to be available on standby only after a valid ID is entered (*Always* or *Disable*).
  - **OK Pressed**: Set the device sensor to be available on standby only after the OK key is pressed *(Always* or *Disable*).
- **Operation Mode**: For each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.
  - **Fingerprint Only**: Set the device to require fingerprint only authorization (*Always*, *Disable*, or Custom Schedule).
  - **Password Only**: Set the device to require password only authorization (*Always*, *Disable*, or Custom Schedule).
  - **Fingerprint/Password**: Set the device to require fingerprint or password authorization (*Always*, *Disable*, or Custom Schedule).
  - **Fingerprint+Password**: Set the device to require fingerprint plus password authorization (*Always*, *Disable*, or Custom Schedule).
  - **Card Only**: Set the device to require only card authorization (*Always*, *Disable*, or Custom Schedule).
  - **Private Auth**: Set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
- **Mifare**
  - **Not Use Mifare**: Check this box to disable MIFARE card authorization.
  - **Use Template on Card**: Check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout:** Click this button to configure the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be

processed in its original form. If “Wiegand” is selected, devices will interpret card ID data according to the Wiegand format settings.

- **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
- **Bit Order:** Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).
- In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.

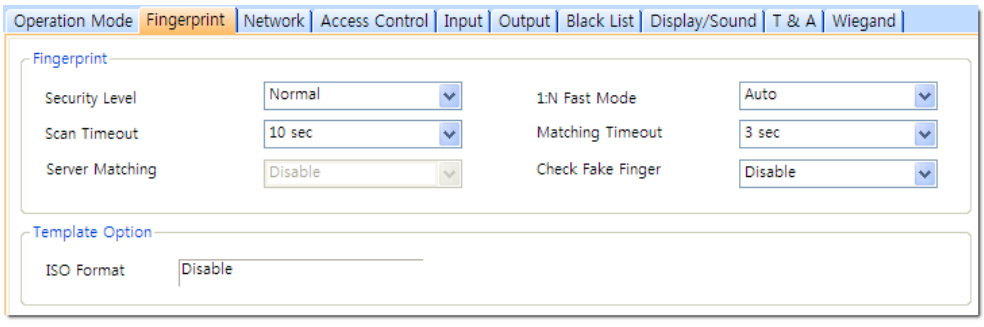
Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

– Use Wiegand Card Bypass: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

5.1.3.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for BioLite Net devices.

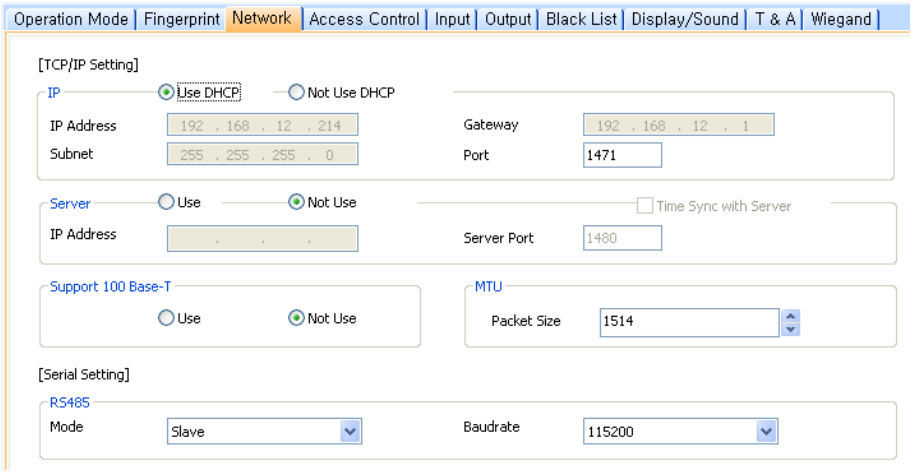


- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.

- **Scan Timeout:** Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
- **Server Matching**: Enable this setting to perform fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
- **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match (*0 [Infinite]* to *10 sec*).
- **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.

5.1.3.3 Network tab

The Network tab allows you to customize network and server settings for BioLite Net devices.



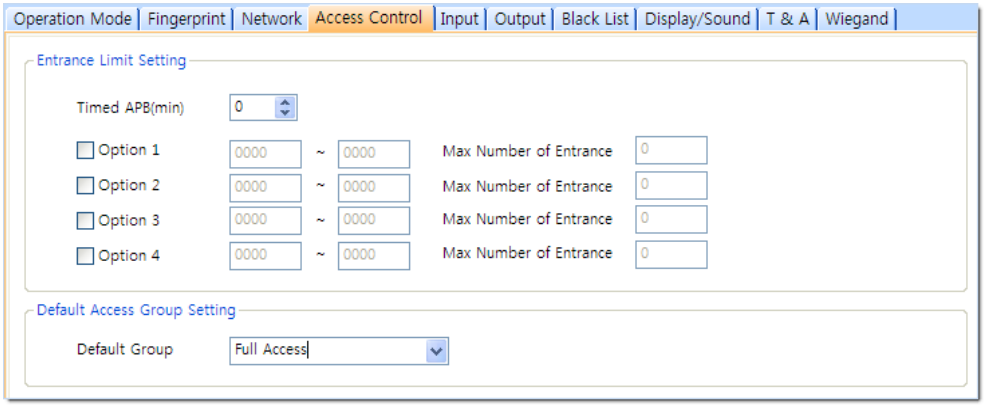
- Support MTU Size setting
  - Devices affiliated with Black Fin support MTU Size setting. The supported packet size is between 1078 and 1514, and the default is 1514.
    (This feature is supported from the FW versions, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.)
- **TCP/IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet**: Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Port:** Specify a port to use for the device.
- **Server**
  - **Use**: Click this option button to use specific server settings.
  - **Not Use**: Click this option button to disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Time Sync with Server:** Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **Support 100 Base-T:** This option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.

- **Use**: Click this option button to enable the 100base-T connection for the device.
- **Not Use**: Click this option button to disable the 100base-T connection for the device.

- **RS485**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.3.4 Access Control tab

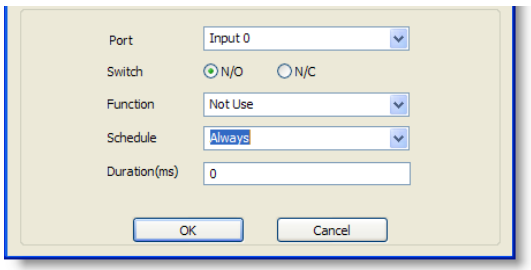
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioLite Net device.



- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance:** Set the maximum number of entries allowed during the specified time limit.
- **Default Access Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.3.5 Input tab

The input tab lists input settings you have specified for a BioLite Net device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.

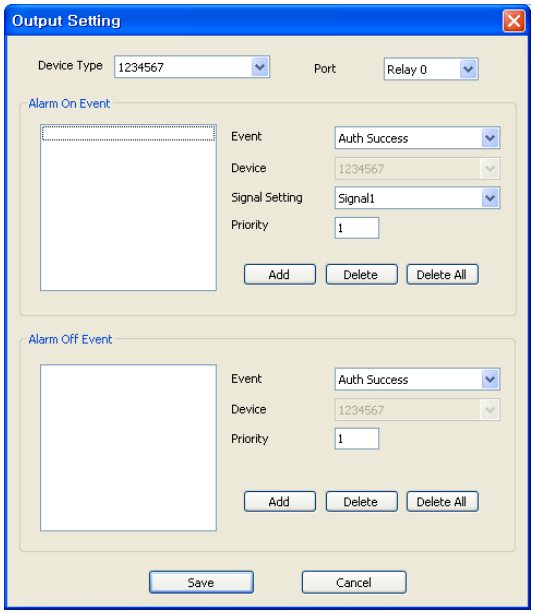


- **Device**: Select the BioLite Net (or Secure I/O) device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - *Not Use*: The input port will not be monitored.
  - *Generic Input*: The input port will be monitored for a triggering action (For the events specified with "Detect Input 1-3" in the **Output setting** dialog box, please see section 5.1.3.6).
  - *Emergency Open*: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - *Release All Alarms*: Cancel alarms associated with this device.
  - *Restart Device*: Restart the device.
  - *Disable Device*: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioLite Net device.
    With BioStar 1.8v, LED Green Input, LED Red Input, Buzzer Input, Access Granted Input, and Access Denied Input were newly added. And these input options are available only with BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), and Xpass (FW 1.3v).

- **Schedule**: Set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.3.6 Output tab

The Output tab lists output settings you have specified for a BioLite Net device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.



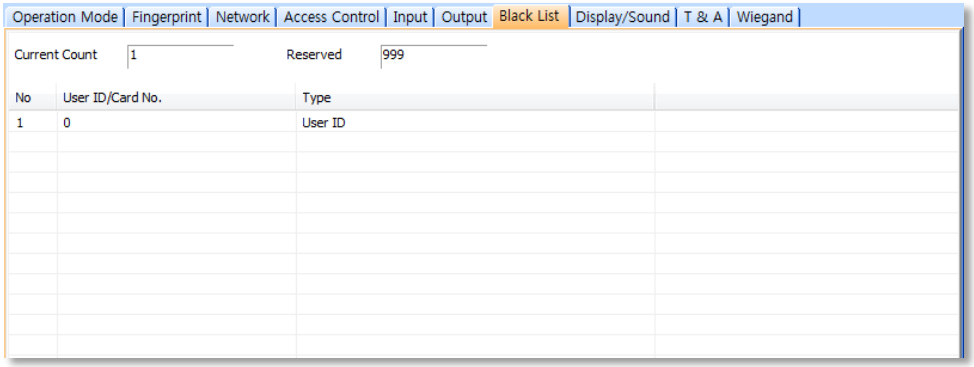
- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: Select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device:** Select the device to monitor for an alarm event.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be

canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.3.7 Black List tab

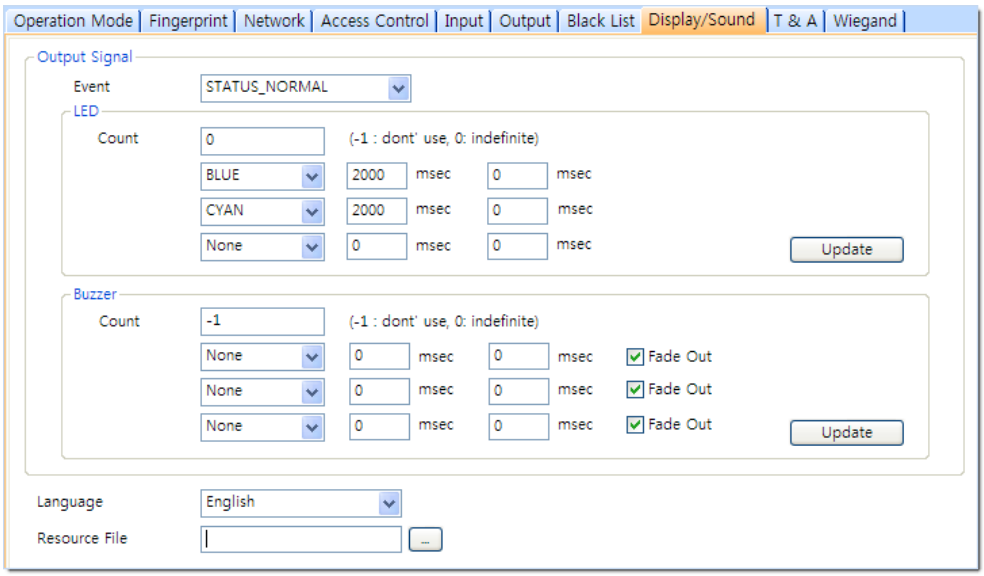
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of user IDs and access cards that have been registered.
- **Reserved** : The remaining number of user IDs and access cards that can be registered.

5.1.3.8 Display/Sound tab

The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event. You can also customize the language used on the device display.

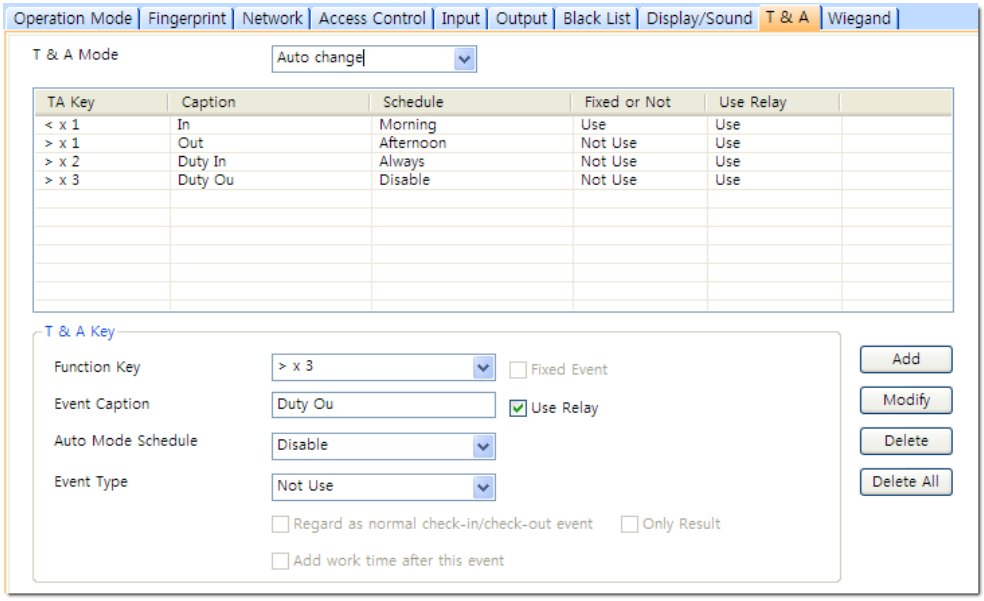


- **Event**: Specify the affected event by selecting it from the drop-down list.
- **LED:** Set the LED behavior for a specified event.
  - **Count**: Enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.
  - **Colors**: Specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer**: Set the buzzer behavior for a specified event.
  - **Count**: Enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume**: Set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out**: Set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.
- **Language:** Set the language to use on the display (*Korean*, *English*, or *Custom*).

- **Resource File:** Set the language resource file to use for the BioStar interface by clicking the ellipsis (…) button and locating the resource file.

5.1.3.9 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioLite Net device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

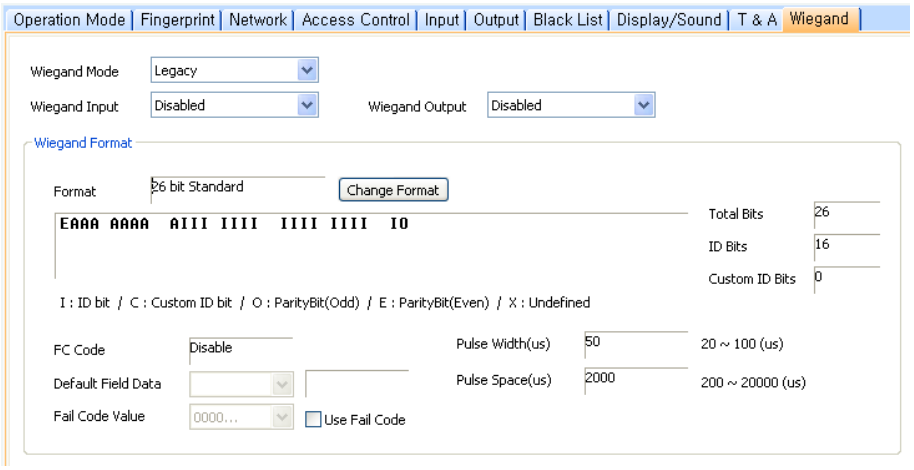


- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key**: Select a function key from the drop-down list to assign a T&A event (**1-*15*). If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption**: Enter a caption for the event.
  - **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, please see section 3.7.1.

– **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users using the appropriate keys will be regarded arriving or leaving on time at work even though they actually come late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users using the appropriate key will be considered working for the remainder of the time slot even though they leave the office early.

5.1.3.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioLite Net device. Unlike BioStation devices, only one Wiegand format can be configured at a time (either input only or output only). You can click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for a BioLite Net device, you can select the checkbox at the top right of the tab. For more information on configuring the Wiegand format, pleaes see section 3.2.16.



- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will process ID data from networked devices and RF card readers in the same way (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input**: Assign the Wiegand input:
  – **Disabled**: The input will not be used.

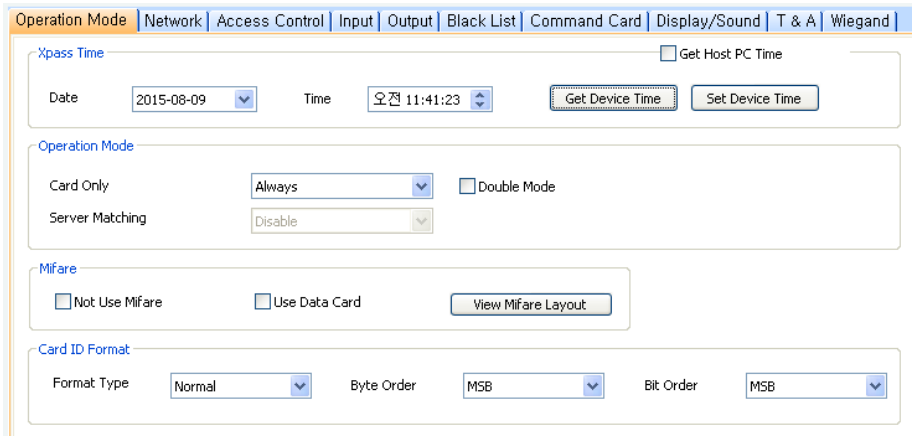
  - **Wiegand [Card]**: The ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]**: The ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output**: Assign the Wiegand output:
  - **Disabled**: The output will not be used.
  - **Wiegand [Card]**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.4 Customize Settings for Xpass Devices

The sections below describe the settings available for Xpass devices. Customize the way Xpass devices function by changing these settings to suit your particular environment and operational needs.

5.1.4.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for Xpass devices.



- **Xpass Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time:** Manually set the device time.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time:** Set the time on the device.
- **Operation Mode**: For each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.

- **Card Only:** Set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
- **Server Matching**: Enable this setting to perform card ID matching at the BioStar server, instead of the device. When this mode is enabled, the device will send card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.

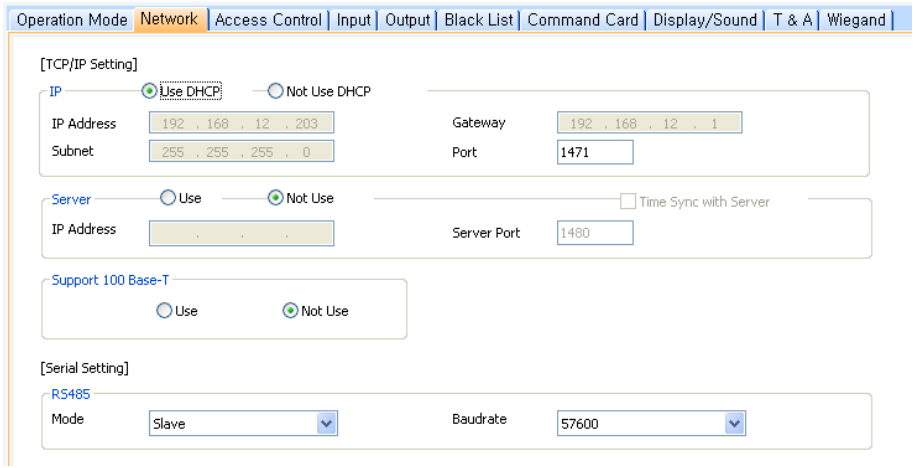
- **Mifare**
  - **Not Use Mifare**: Check this box to disable MIFARE card authorization.
  - **Use Data Card:** Check this box to use the user data on the MIFARE card for authorization. The user data card does not provide fingerprint templates.
  - **View Mifare Layout**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order:** Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

– In Double mode, setting option which includes an administrator is supported. In Double mode, door relay will not open unless an administrator authenticates within 15 seconds after a user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a user or an administrator, authenticate within 15 seconds.
Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

– Use Wiegand Card Bypass: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.
Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

5.1.4.2 Network tab

The Network tab allows you to customize network and server settings for Xpass devices.



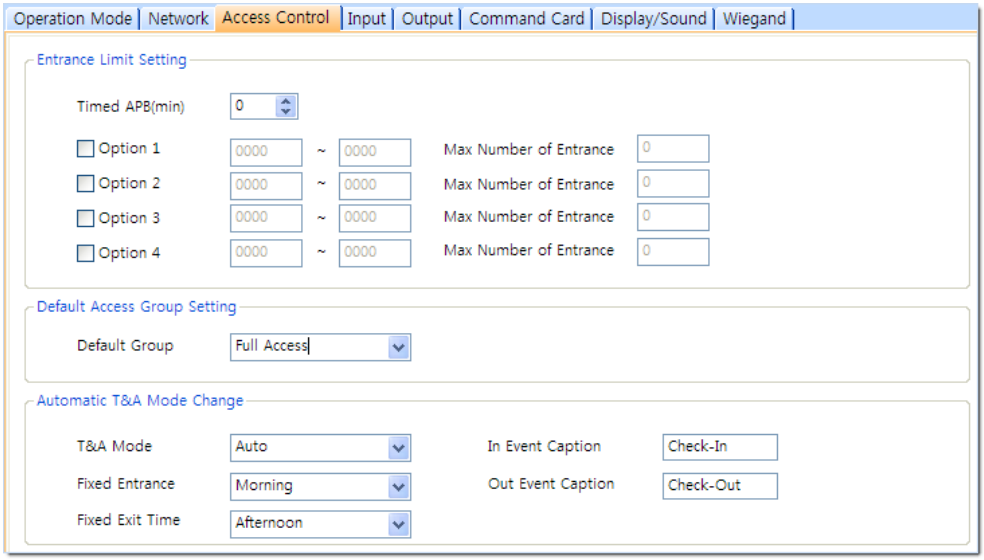
- **TCP/IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet**: Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Port:** Specify a port to use for the device.
- Support MTU Size setting
  - Devices affiliated with Black Fin support MTU Size setting. The supported packet size is between 1078 and 1514, and the default is 1514.
    Note: This feature is supported from the FW versions, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.
- **Server**
  - **Use**: Click this option button to use specific server settings.
  - **Not Use**: Click this option button to disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **Support 100 Base-T**: This option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.

- **Use**: Click this option button to enable the 100base-T connection for the device.
- **Not Use**: Click this option button to disable the 100base-T connection for the device.

- **RS485**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.4.3 Access Control tab

The Access Control tab allows you to customize entrance limit settings, default access groups, and T&A mode settings for Xpass devices.



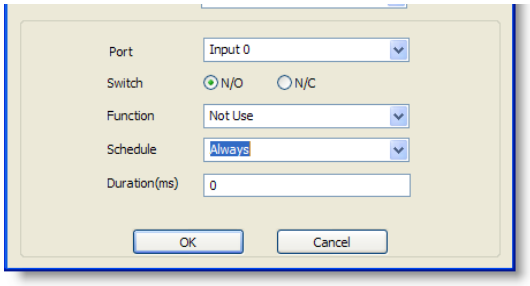
- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance:** Set the maximum number of entries allowed during the specified time limit.
- **Default Access Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.
- Automatic T&A Mode Change
  - **T&A Mode**: Set the time and attendance mode for the device (*Disable*, *Fixed In*, *Fixed Out*, and *Auto*).
  - **Fixed Entrance**: When the "Auto" T&A mode is selected, specify when to allow entrance events by selecting a timezone (*Always*, *Disable*, or

custom timezone) in the drop-down list. For more information on creating a timezone, please see section 3.7.1.

- **Fixed Exit Time**: When the "Auto" T&A mode is selected, specify when to allow exit events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
- **In Event Caption**: Set a caption for check-in.
- **Out Event Caption**: Set a caption for check-out.

5.1.4.4 Input tab

The input tab lists input settings you have specified for an Xpass device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.



- **Device**: Select the Xpass (or Secure I/O) device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch:** Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input**: The input port will be monitored for a triggering action (For the events specified with "Detect Input 1-3" in the **Output setting** dialog box, please see section 5.1.4.5).
  - **Emergency Open**: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device:** Restart the device.
  - **Disable Device:** Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter

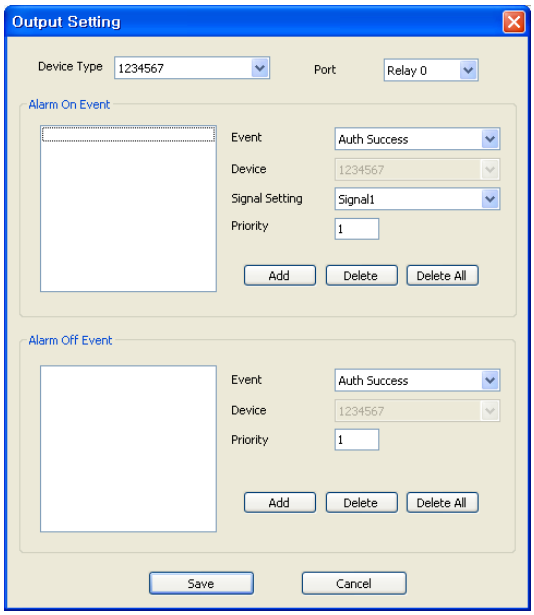
the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.

– With BioStar 1.8v, LED Green Input, LED Red Input, Buzzer Input, Access Granted Input, and Access Denied Input were newly added. And these input options are available only with BioStation (FW 1.93v), BioStation T2 (FW 1.3v), FaceStation (FW 1.3v), BioEntry Plus (FW 1.6v), BioEntry W (FW 1.2v), BioLite Net (FW 1.4v), and Xpass (FW 1.3v).

- **Schedule**: Set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.4.5 Output tab

The Output tab lists output settings you have specified for an Xpass device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  – **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance*

Limited, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).

- **Device:** Select the device to monitor for an alarm event.
- **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

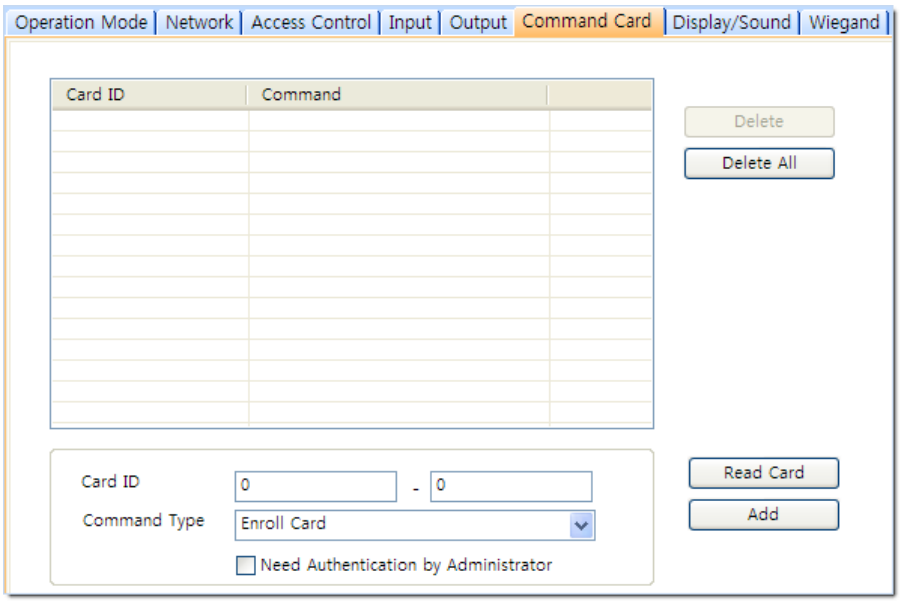
- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.4.6 Blacklist

From BioStar 1.8, 'Blacklist' feature is supported with Xpass.
(This feature is available only with FW 1.3v or higher.)

5.1.4.7 Command Card tab

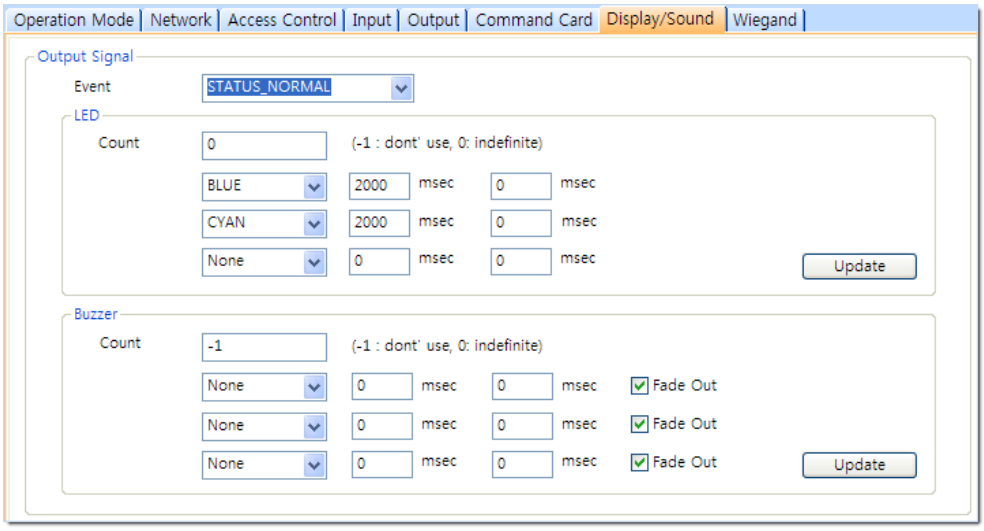
The Command Card tab allows you to issue command cards. For more information about command cards, please see section 3.2.8.1.



- **Card ID**: Enter the card ID or click **Read Card** and place a command card on the reader to automatically populate the fields.
- **Command Type**: Select a type of command card to issue (*Enroll Card*, *Delete Card*, or *Delete All Card*).

5.1.4.8 Display/Sound tab

The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



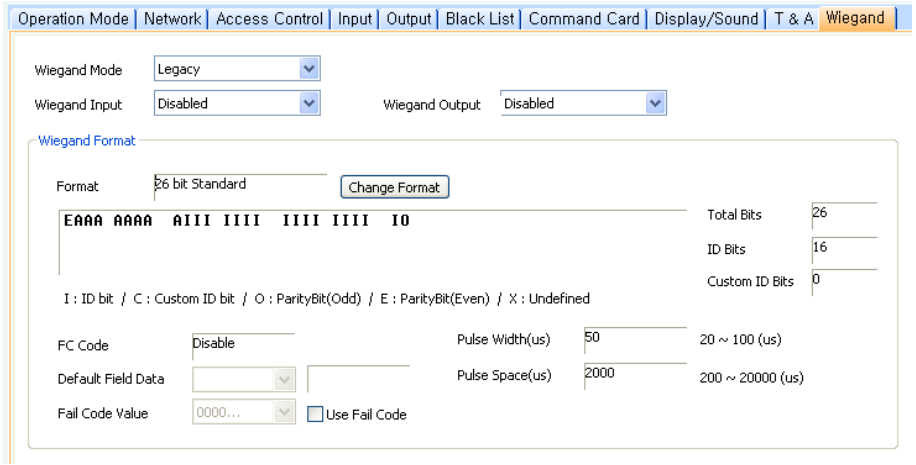
- **Event**: Specify the affected event by selecting it from the drop-down list.
- **LED**: Set the LED behavior for a specified event.
  - **Count**: Enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.
  - **Colors**: Specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom.

Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.

- **Buzzer**: Set the buzzer behavior for a specified event.
  - **Count**: Enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume**: Set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out**: Set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.4.9 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for an Xpass device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for an Xpass device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.16



- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input**: Assign the Wiegand input:
  - **Disabled**: The input will not be used.
  - **Wiegand [Card]**: The ID field of the Wiegand string is interpreted as a card ID.

- **Wiegand [User]**: The ID field of the Wiegand string is interpreted as a user ID.

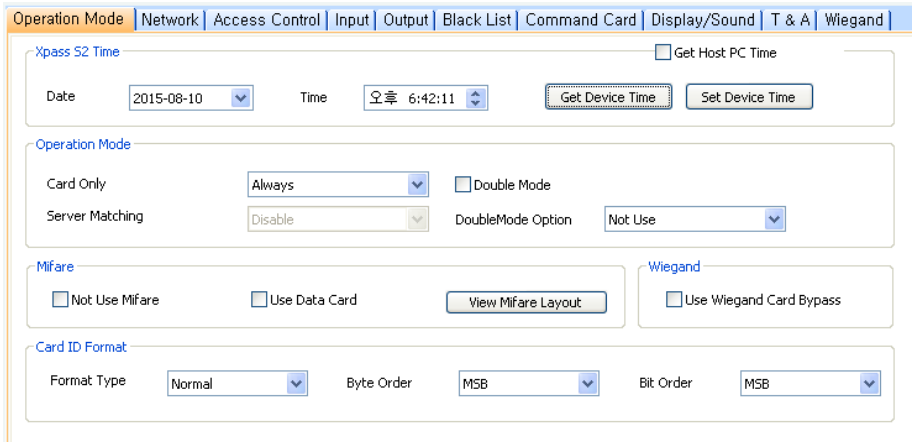
- **Wiegand Output**: Assign the Wiegand output:
  - **Disabled**: The output will not be used.
  - **Wiegand [Card]**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.5 Customize Settings for Xpass S2 Devices

The sections below describe the settings available for Xpass S2 devices. Customize the way Xpass S2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.5.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for Xpass S2 devices.



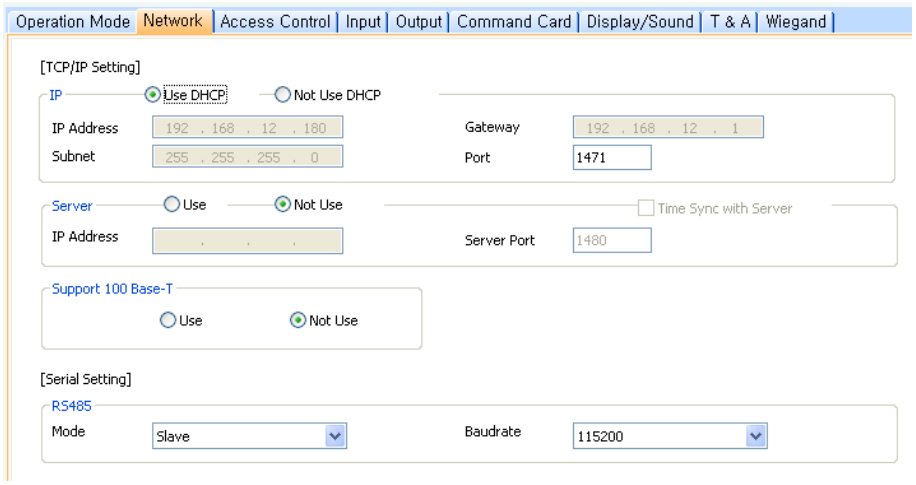
- **Xpass S2 Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time:** Manually set the device time.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time:** Set the time on the device.
- **Operation Mode**: For each of the following options, click the corresponding checkbox to enable Double Verification Mode, which requires verification of two users' credentials to gain entry to a door.

- **Card Only:** Set the device to require only card authorization (*Always*, *Disable*, or custom schedule).
- **Server Matching**: Enable this setting to perform card ID matching at the BioStar server, instead of the device. When this mode is enabled, the device will send card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.

- **Mifare**: Mifare template cards are not supported in the Xpass S2 device.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order**: Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.5.2 Network tab

The Network tab allows you to customize network and server settings for Xpass S2 devices.

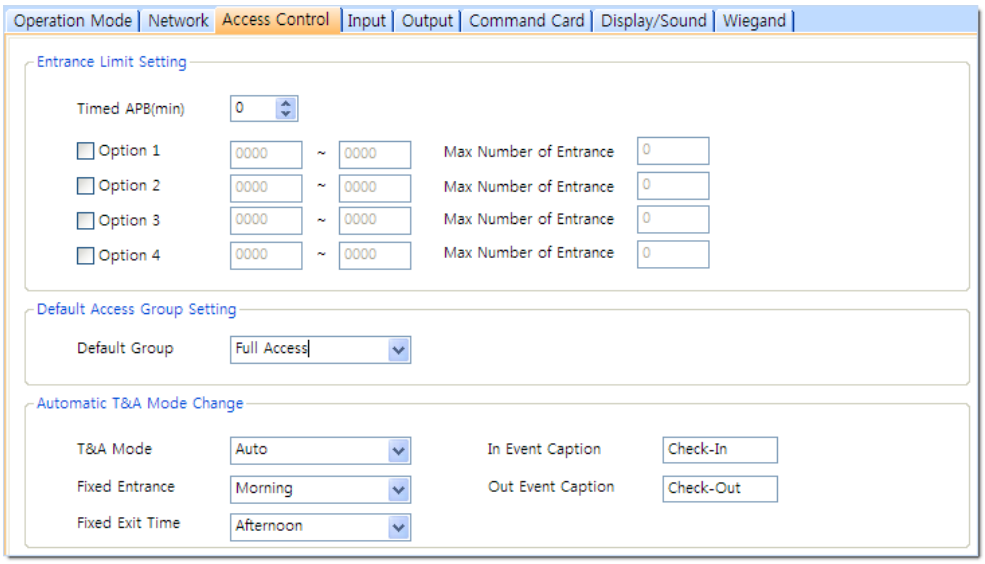


- **TCP/IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP**: Specify an IP address for the device.
  - **Subnet**: Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Port:** Specify a port to use for the device.

- **Server**
  - **Use**: Click this option button to use specific server settings.
  - **Not Use**: Click this option button to disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **Support 100 Base-T:** This option allows you to enable or disable a fast Ethernet connection for the device. When enabled, the device will detect the Ethernet network and automatically establish the best connection. If you do not enable this option, the device will attempt to establish a 10Base-T Ethernet connection.
  - **Use**: Click this option button to enable the 100base-T connection for the device.
  - **Not Use**: Click this option button to disable the 100base-T connection for the device.
- **RS485**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*).
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.5.3 Access Control tab

The Access Control tab allows you to customize entrance limit settings, default access groups, and T&A mode settings for Xpass S2 devices.



- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has

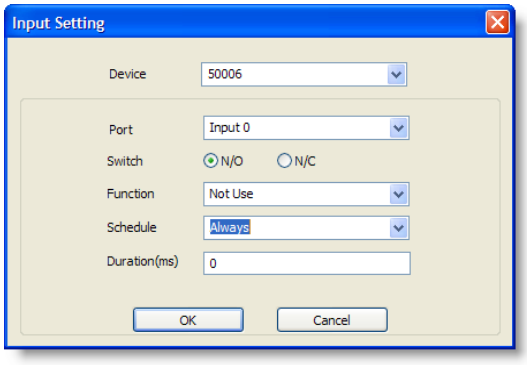
gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.

- **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
- **Max Number of Entrance**: Set the maximum number of entries allowed during the specified time limit.

- **Default Access Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.
- Automatic T&A Mode Change
  - **T&A Mode**: Set the time and attendance mode for the device (*Disable*, *Fixed In*, *Fixed Out*, and *Auto*).
  - **Fixed Entrance**: When the "Auto" T&A mode is selected, specify when to allow entrance events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
  - **Fixed Exit Time**: When the "Auto" T&A mode is selected, specify when to allow exit events by selecting a timezone (*Always*, *Disable*, or custom timezone) in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
  - **In Event Caption**: Set a caption for check-in.
  - **Out Event Caption**: Set a caption for check-out.

5.1.5.4 Input tab

The input tab lists input settings you have specified for an Xpass S2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.

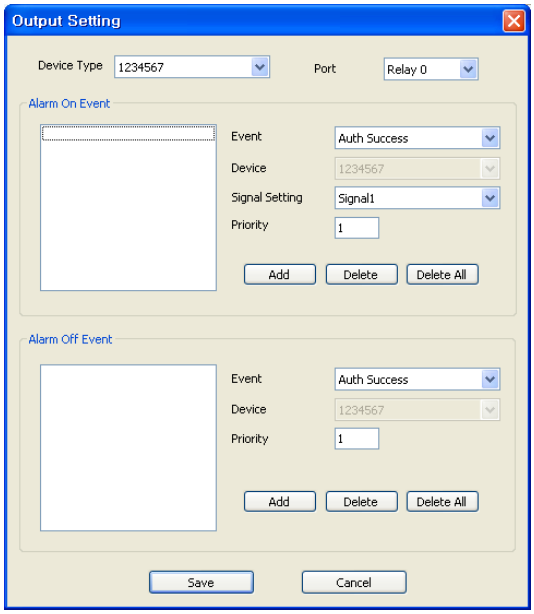


- **Device**: Select the Xpass S2 (or Secure I/O) device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, the following options are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.

- **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input**: The input port will be monitored for a triggering action (events specified with "Detect Input 1-3" in the **Output Setting** dialog box —see section 5.1.5.5).
  - **Emergency Open**: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device:** Restart the device.
  - **Disable Device:** Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must enter the master password for a BioStation device or provide authentication locally for a BioEntry Plus or BioEntry W device.
- **Schedule**: Set the schedule for the input actions (*Always*, *Disable*, or custom schedule).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.5.5 Output tab

The Output tab lists output settings you have specified for an Xpass device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.

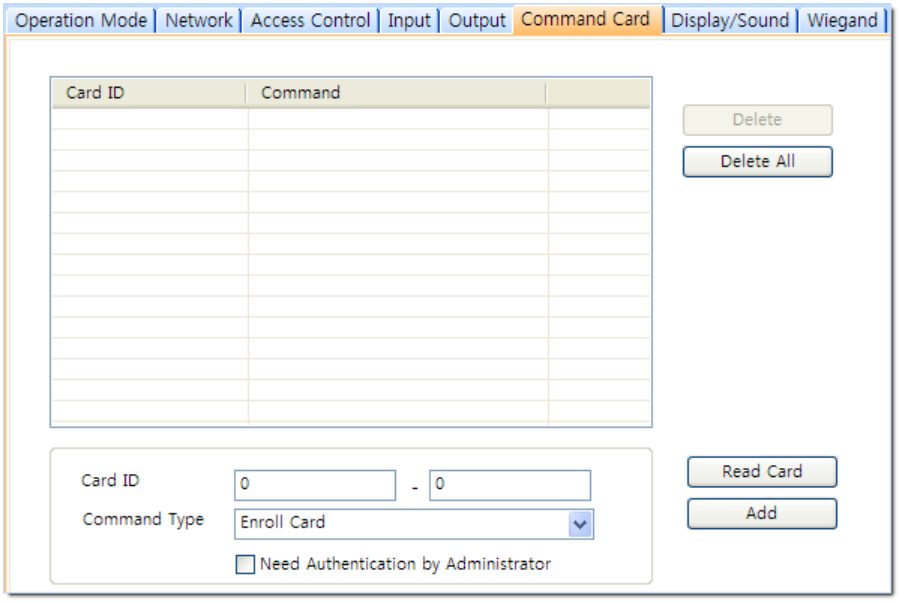


- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: Select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device:** Select the device to monitor for an alarm event.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.

- **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
- **Device**: Select the device to monitor for an alarm event.
- **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on event (activate) can be overridden only by an alarm off (deactivate) event with a priority of 1 or 2.

5.1.5.6 Command Card tab

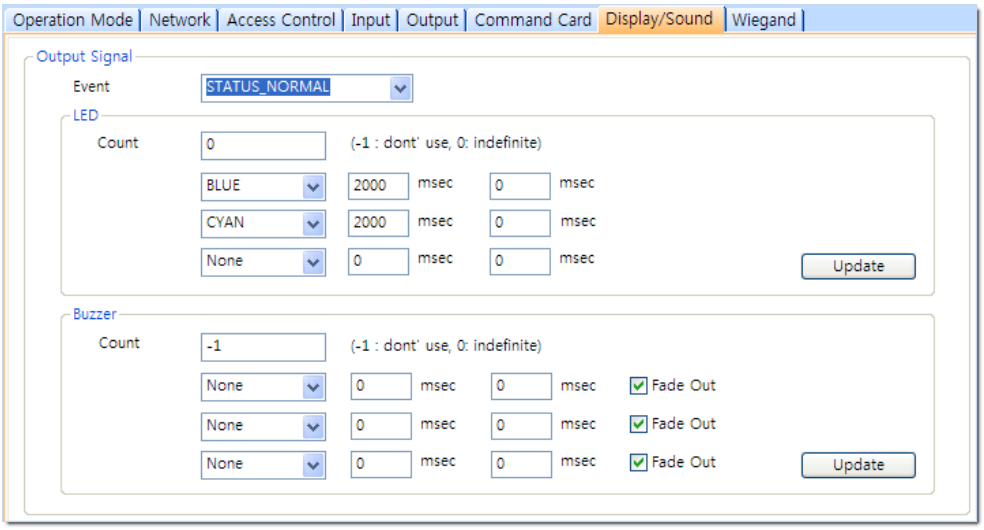
The Command Card tab allows you to issue command cards. For more information about command cards, see section 3.2.8.1.



- **Card ID**: Enter the card ID or click **Read Card** and place a command card on the reader to automatically populate the fields.
- **Command Type**: Select a type of command card to issue (*Enroll Card*, *Delete Card*, or *Delete All Card*).

5.1.5.7 Display/Sound tab

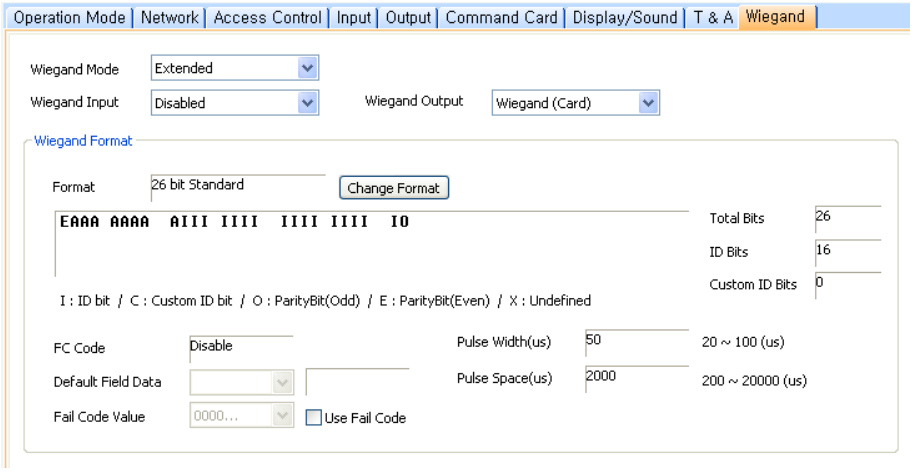
The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



- **Event**: Specify the affected event by selecting it from the drop-down list.
- **LED:** Set the LED behavior for a specified event.
  - **Count**: Enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.
  - **Colors**: Specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer**: Set the buzzer behavior for a specified event.
  - **Count**: Enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume**: Set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
  - **Fade Out**: Set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.5.8 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for an Xpass device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for an Xpass device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.16.



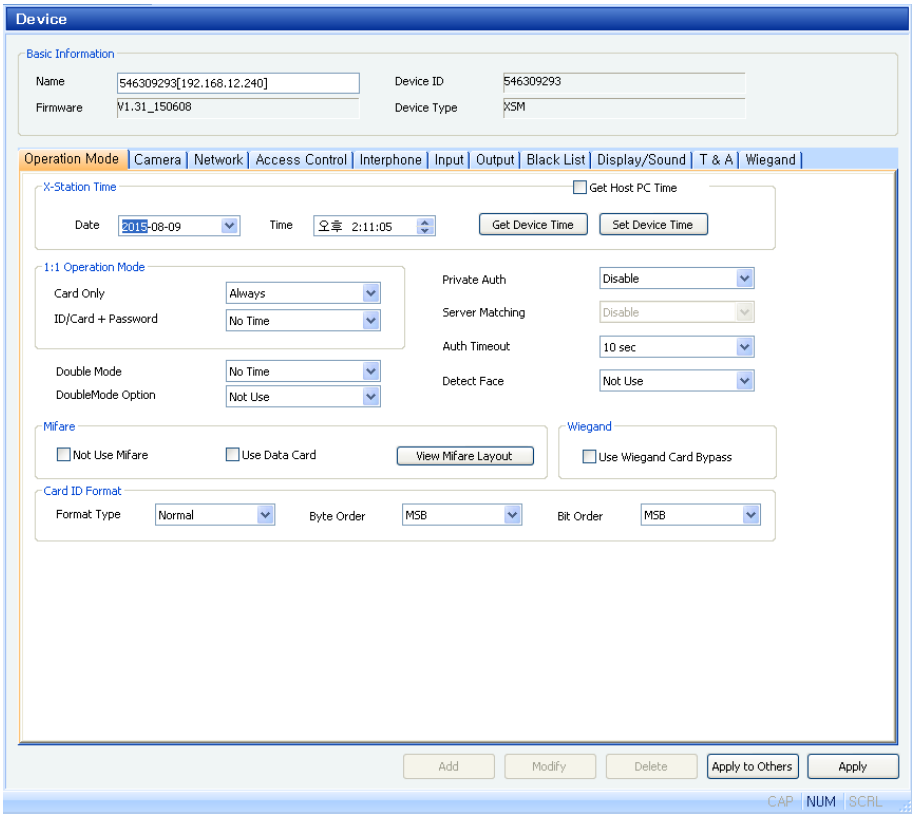
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand Input**: Assign the Wiegand input:
  - **Disabled**: The input will not be used.
  - **Wiegand [Card]**: The ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand [User]**: The ID field of the Wiegand string is interpreted as a user ID.
- **Wiegand Output**: Assign the Wiegand output:
  - **Disabled**: The output will not be used.
  - **Wiegand [Card]**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand [User]:** Inserts the user ID of the authenticated user in the ID field of the Wiegand string.

5.1.6 Customize Settings for X-Station Devices

The sections below describe the settings available for X-Station devices. Customize the way X-Station devices function by changing these settings to suit your particular environment and operational needs.

5.1.6.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for X-Station devices.



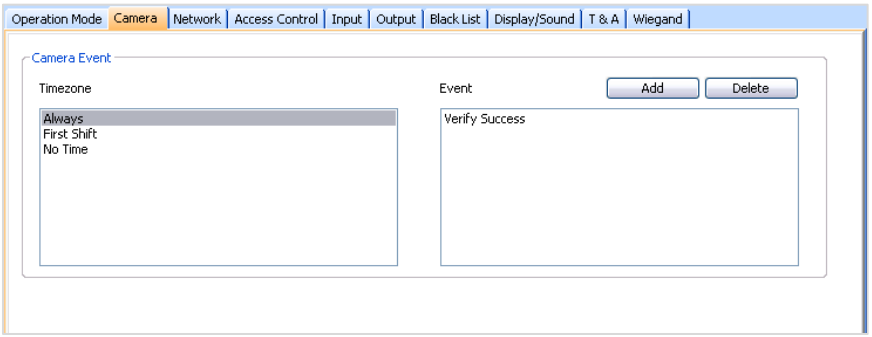
- **X-Station Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time:** Manually set the device time.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **1: 1 Operation Mode**: The drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **Card Only**: Set the device to require only card authorization (*No Time, First Shift, or Always*).

  - **ID/Card + Password**: Set the device to require ID or card plus password authorization (*No Time, First Shift, or Always*).
- **Private Auth**: Set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
- **Double Mode**: Set the device to require authentication of two users' access cards or fingerprints (*Always*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.
- **Server Matching**: Enable this setting to perform card ID matching at the BioStar server, instead of the device. When this mode is enabled, the device will send card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Auth Timeout**: Set the length of time before the device will timeout when trying to identify an ID match (*5, 10, 15, 20, or 30 sec*).
- **Detect Face**: Set the device to capture a face image. Upon successful authentication, the captured image is stored in the event log and can be used later for verification purposes.
- **Mifare**
  - **Not Use Mifare**: Check this box to disable MIFARE card authorization.
  - **Use Data Card:** Check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order**: Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.6.2 Camera tab

The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click

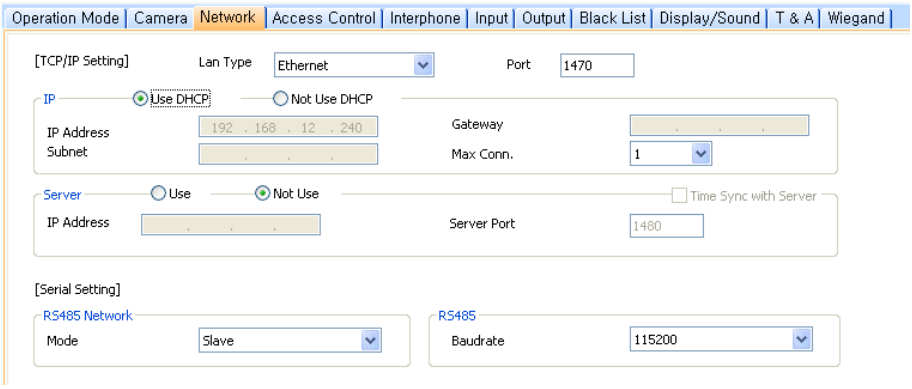
Add to select an event that will activate the camera. Click **Apply** to save your settings.



Attention: We recommend that add the authentication events to the camera event for security. Add only a maximum of 30 events to reduce the network load between the device and the server.

5.1.6.3 Network tab

The Network tab allows you to customize network and server settings for X-Station devices.

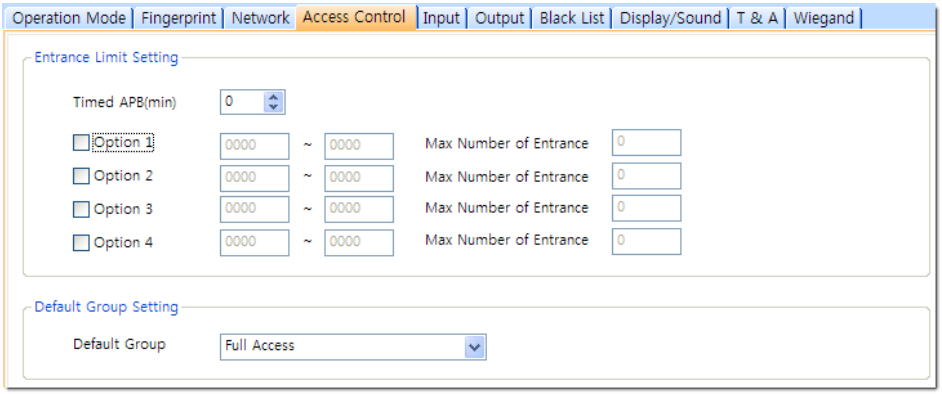


- **TCP/IP Setting**
  - **LAN Type:** Select a type of LAN connection from the drop-down list (*Disable*, or *Ethernet*).
  - **Port**: Specify a port to use for the device.
- **IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet**: Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Max Conn.**: Specify the maximum number of connections to allow.

- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port**: Specify the port used to connect to the server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
- **RS485**
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.6.4 Access Control tab

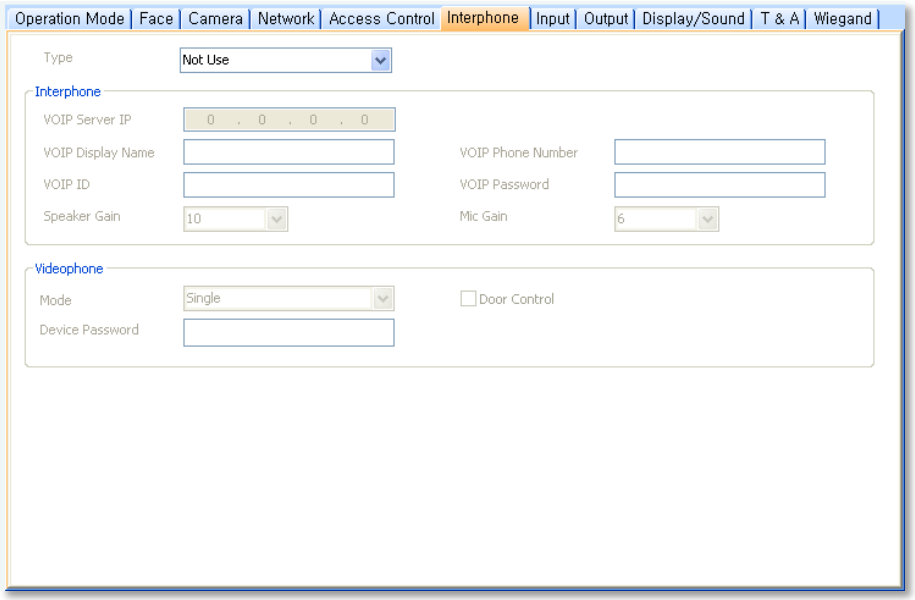
The Access Control tab allows you to customize entrance limit settings and default access groups for an X-Station device.



- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance**: Set the maximum number of entries allowed during the specified time limit.
- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.6.5 Interphone tab

The Interphone tab allows you to set the device to act as an interphone to allow communication between people on either side of the door.



- **Type**: Select one of the following options:
  - **Analogue Interphone**: Choose this option to enable the analogue interphone.
  - **IP Interphone**: Choose this option to enable the VoIP feature. A telephone is required.
  - **BioStar Videophone**: Choose this option to enable the videophone feature that supports both video and voice calls. The supplied PC software is required. The BioStar videophone works only with the device firmware version of FaceStation V1.0 or later.

When you select **IP Interphone** in the Type drop-down list, specify the following settings:

- **VOIP Server IP**: Specify an IP address for VOIP server.
- **VoIP Display Name**: Specify a name to use for communication through the interphone.
- **VoIP Phone Number**: Specify a phone number for the interphone.
- **VoIP ID**: Specify a user name to access the VoIP server.
- **VoIP Password**: Specify a password to access the VoIP server.
- **Speaker Gain**: Specify the volume of the speaker.
- **Mic Gain**: Specify the volume of the microphone.

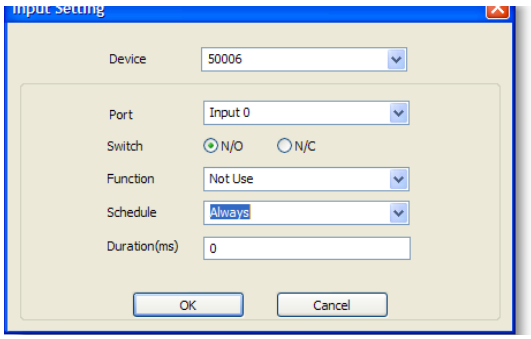
When you select **Videophone** in the Type drop-down list, specify the following settings:

- **Mode**: Specify the videophone purpose (*Single* or *Extension*).
- **Door Control**: Check this option if the videophone is used for door access.

- **Device Password**: Enter the videophone device password.

5.1.6.6 Input tab

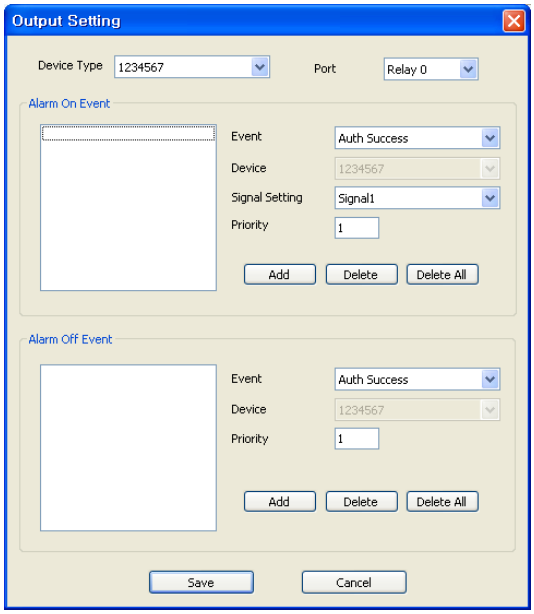
The input tab lists input settings you have specified for an X-Station device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.



- **Device**: Select the X-Station device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input**: The input port will be monitored for a triggering action (For the events specified with “Detect Input 0-3” in the **Output Setting** dialog box, please see section 5.1.1.6).
  - **Emergency Open**: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a “Close Door” command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.
- **Schedule**: Set the schedule during which the inputs will be monitored (*Always, First Shift, or No Time*).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.6.7 Output tab

The Output tab lists output settings you have specified for an X-Station device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.

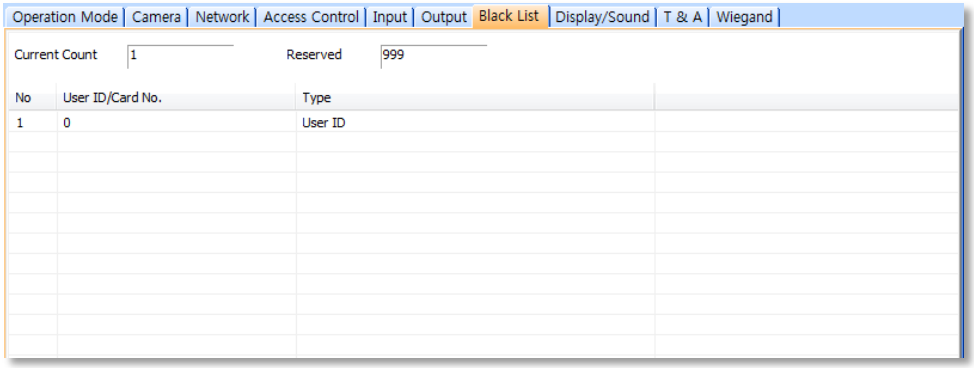


- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Closed*, *Forced Open Door*, *Held Open Door*, *Detect Input #0-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.
- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.

- **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
- **Device**: Select the device to monitor for an alarm event.
- **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off” (deactivate) event with a priority of 1 or 2.

5.1.6.8 Black List tab

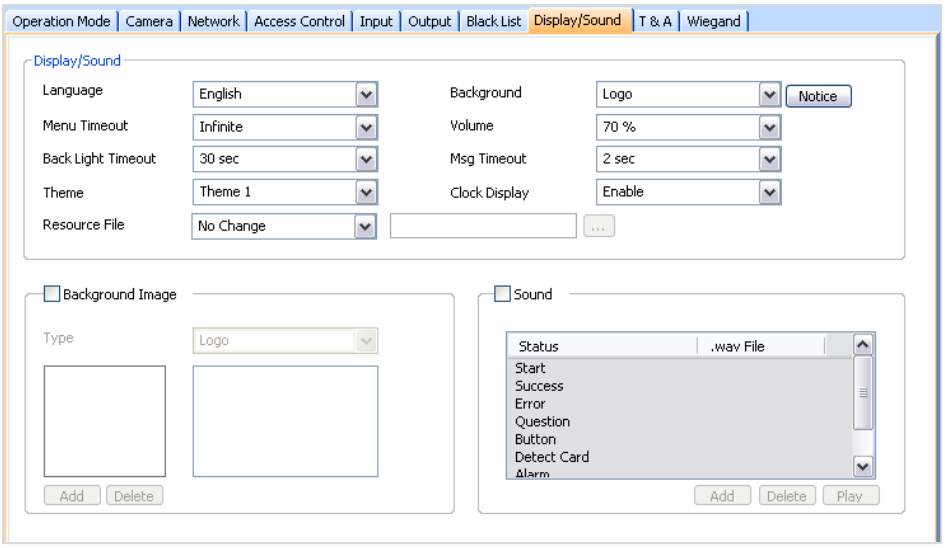
The Black list tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of user IDs and access cards that have been registered.
- **Reserved**: The remaining number of user IDs and access cards that can be registered.

5.1.6.9 Display/Sound tab

The Display/Sound tab allows you to customize the X-Station display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



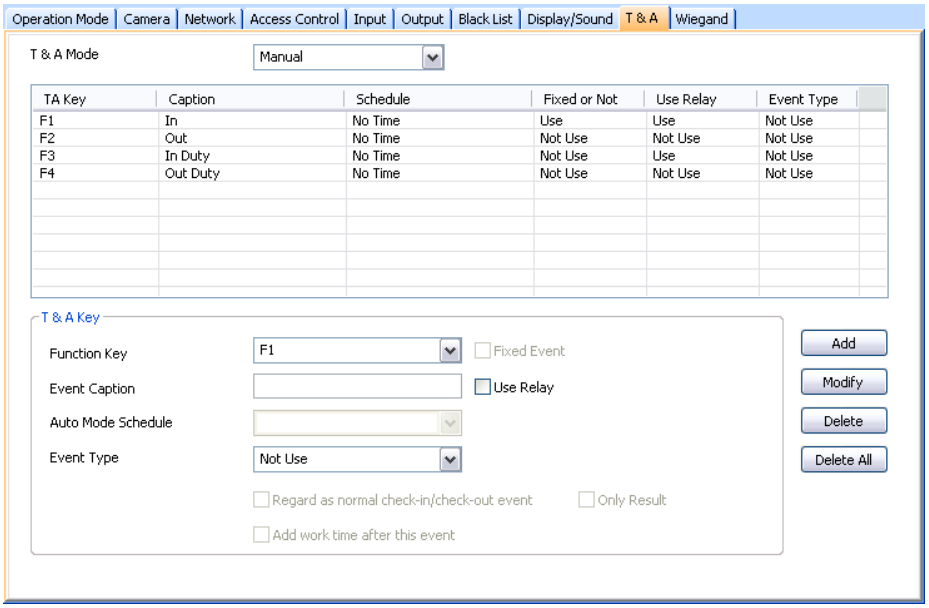
- **Display/Sound**
  - **Language**: Set the language to use on the display (Korean, English, or Custom).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen.
  - **Back Light Timeout**: Set the length of time before the display goes dim (*Infinite*, *10*, *20*, *30*, *40*, *50*, or *60 sec*).
  - **Theme**: Set a display theme (*Theme 1-3*).
  - **Resource File**: Set the language resource file to use for the X-Station interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the X-Station display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 240x320 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
  - **Notice**: Click this button to create a notice that will be shown on the X-Station display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
  - **Volume**: Set the volume of the X-Station device (*0%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed.

- **Clock Display**: Set to display the current time on the device (Enable or Disable).

- **Background Image**: Click this checkbox to upload new background images. Click **Add** to locate and add a new image file. To delete an existing image, click the image name and then click **Delete**.
  - **Type**: Set the type of background for the X-Station display (*Logo, Notice, or Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 240x320 pixels for Notices and 240x320 pixels for Logos. Only one image at a time can be used as a logo or notice.
- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click **Add** to locate and add a new sound file. Click **Delete** to remove custom sound files or **Play** to preview a custom sound file.

5.1.6.10 T&A tab

The T&A tab allows you to configure the mode and key settings for an X-Station device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

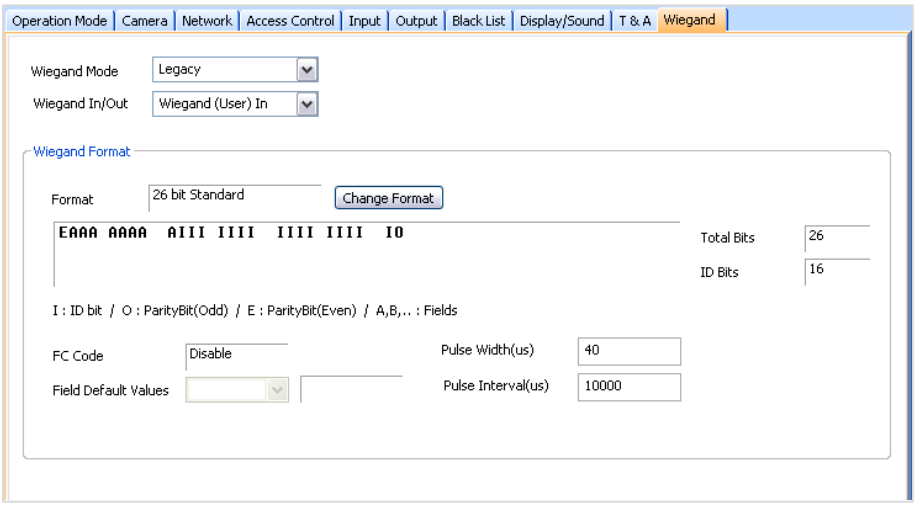


- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual**: Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.

- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key**: Select a function key from the drop-down list to assign a T&A event (**1-*15*). If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption**: Enter a caption for the event.
  - **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.7.1.
  - **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users using the appropriate keys will be regarded arriving or leaving on time at work even though they actually come late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users using the appropriate key will be considered working for the remainder of the time slot even though they leave the office early.

5.1.6.11 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for an X-Station device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, please see section 3.2.16.



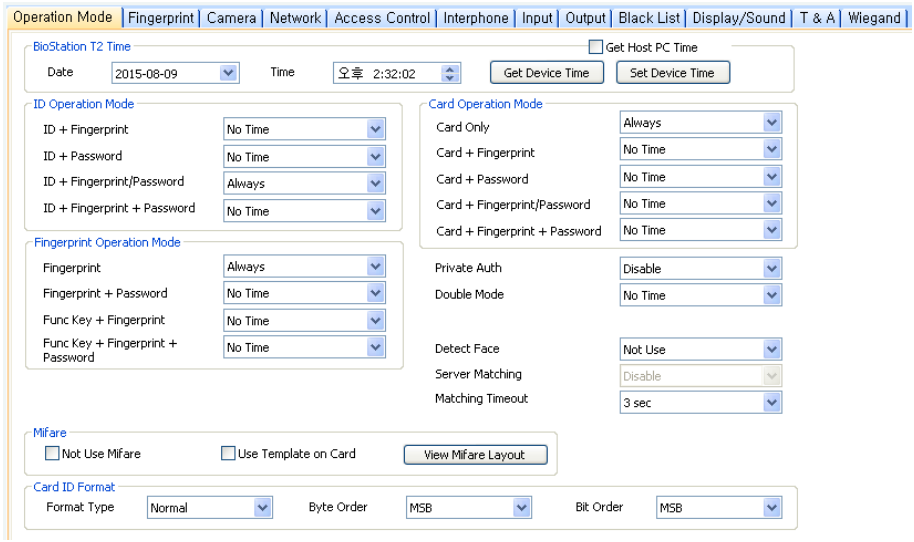
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will process ID data from networked devices and RF card readers in the same way (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the function of the Wiegand input or output:
  - **Wiegand (User) In**: The ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand (User) Out**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand (Card) Out**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.1.7 Customize Settings for BioStation T2 Devices

The sections below describe the settings available for BioStation T2 devices. Customize the way BioStation T2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.7.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation T2 devices.



- **BioStation T2 Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time**: Manually set the device time.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **ID Operation Mode**: The drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID + Fingerprint**: Set the device to require ID plus fingerprint authorization (*Always*, or *No Time*).
  - **ID + Password**: Set the device to require ID plus password authorization (*Always*, or *No Time*).
  - **ID + Fingerprint/Password**: Set the device to require ID plus fingerprint or password authorization (*Always*, or *No Time*).
  - **ID + Fingerprint + Password**: Set the device to require ID plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Card Operation Mode**

  - **Card Only**: Set the device to require only card authorization (*Always*, or *No Time*).
  - **Card + Fingerprint**: Set the device to require card plus fingerprint authorization (*Always*, or *No Time*).
  - **Card + Password**: Set the device to require card plus password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint/Password**: Set the device to require card plus fingerprint or password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint + Password**: Set the device to require card plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Fingerprint Operation Mode**
  - **Fingerprint**: Set the device to require only fingerprint authorization (*Always*, or *No Time*).
  - **Fingerprint + Password**: Set the device to require fingerprint plus password authorization (*Always*, or *No Time*).
  - **Func Key + Fingerprint**: Set the device to require function key plus fingerprint authorization (*Always*, or *No Time*).
  - **Func Key + Fingerprint + Password**: Set the device to require function key plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Other Options**
  - **Private Auth**: Set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
  - **Double Mode**: Set the device to require authentication of two users' IDs, access cards or fingerprints (*Always*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.
  - **Detect Face**: Set the device to capture a face image. Upon successful authentication, the captured image is stored in the event log.
  - **Server Matching**: Enable this setting to perform user ID, fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the user ID, fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).

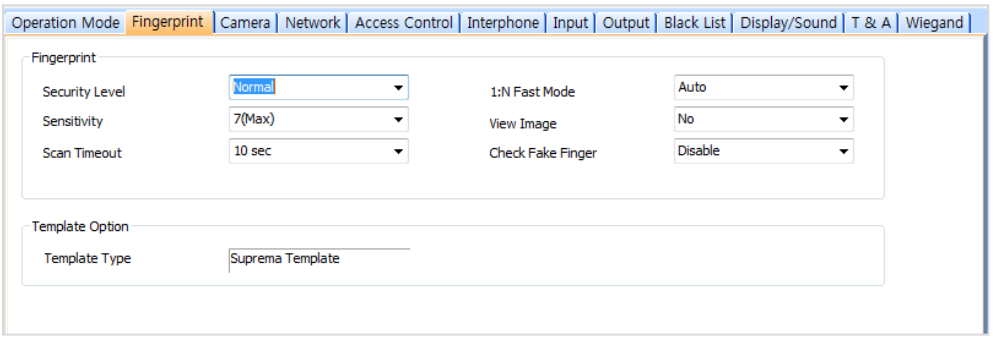
- **Mifare**
  - **Not Use Mifare**: Check this box to disable MIFARE card authorization.
  - **Use Template on Card**: Check this box to use the template on the MIFARE card for authorization.
  - **View Mifare Layout**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order**: Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).
  - In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.

    Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.
  - Use Wiegand Card Bypass: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

    Note: This feature is supported from the FW versions, BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

5.1.7.2 Fingerprint tab

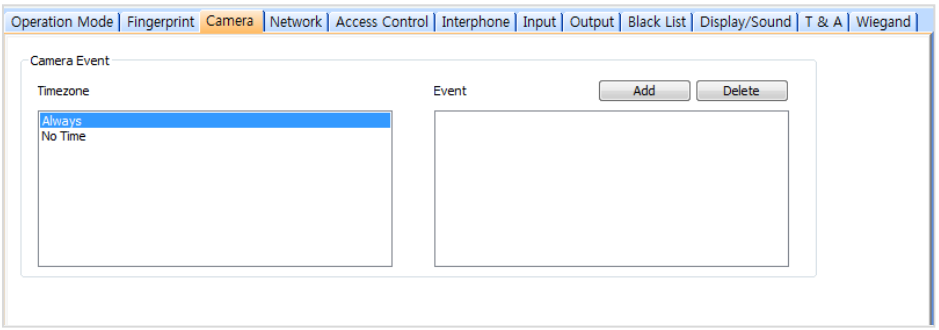
The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation T2 devices.



- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Sensitivity**: Set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **Scan Timeout**: Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **View Image**: Set to show or hide fingerprint images on the BioStation T2 display (*Yes* or *No*).
  - **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.
  - **Template Option**: Displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

5.1.7.3 Camera tab

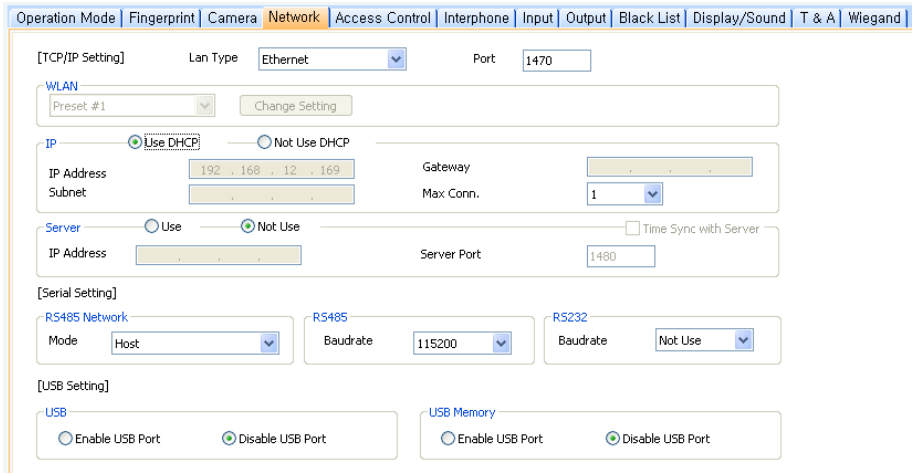
The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



Attention: We recommend that add the authentication events to the camera event for security. Add only a maximum of 30 events to reduce the network load between the device and the server.

5.1.7.4 Network tab

The Network tab allows you to customize network and server settings for BioStation T2 devices.

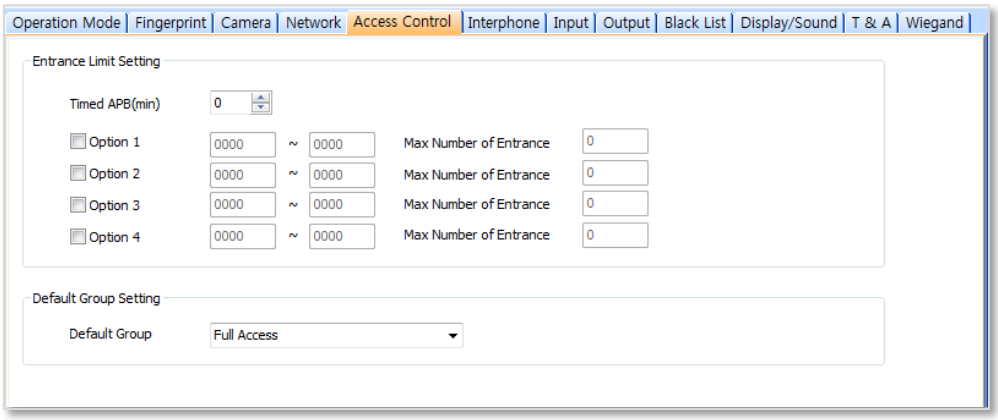


- **TCP/IP Setting**
  - **LAN Type**: Select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port**: Specify a port to use for the device.
- **WLAN**
  - **Change Setting**: Click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.
- **IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.

  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet:** Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Max Conn.**: Specify the maximum number of connections to allow.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port:** Specify the port used to connect to the server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
- **RS485**
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232**
  - **Baudrate**: Set the baud rate for a device connected via RS232 (*9600* to *115200*).
- **USB**: Click the option buttons to enable or disable the USB port on the BioStation T2 device.
- **USB Memory**: Click the option buttons to enable or disable the USB memory on the BioStation T2 device.

5.1.7.5 Access Control tab

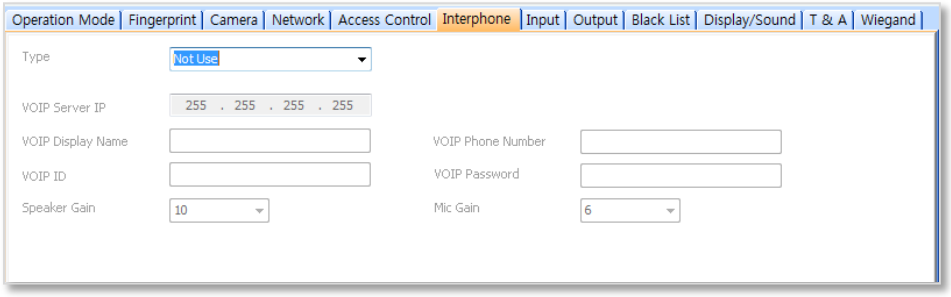
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioStation T2 device.



- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's ID, access card, or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance**: Set the maximum number of entries allowed during the specified time limit.
- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.7.6 Interphone tab

The Interphone tab allows you to set the device to act as an interphone to allow communication between people on either side of the door.



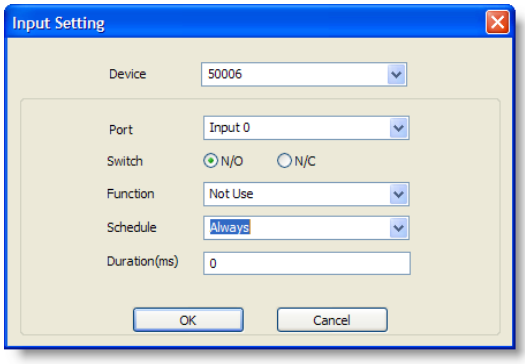
- **Type** – select one of the following options:
  - **Analogue Interphone**: Choose this option to enable the analogue interphone.
  - **IP Interphone**: Choose this option to enable the VoIP feature. A telephone is required.
  - **BioStar Videophone**: Choose this option to enable the videophone feature that supports both video and voice calls. The supplied PC software is required. The BioStar videophone works only with the device firmware version of BioStation T2 V1.1 or later.

When you select **IP Interphone** in the Type drop-down list, specify the following settings:

- **VoIP Server IP**: Specify an IP address for the VoIP server.
- **VoIP Phone Number**: Specify a phone number for the interphone.
- **VoIP Display Name**: Specify a name to use for communication through the interphone.
- **VoIP ID**: Specify a user name to access the VoIP server.
- **VoIP Password**: Specify a password to access the VoIP server.
- **VoIP Speaker Gain**: Specify the volume of the speaker.
- **VoIP Mic Gain**: Specify the volume of the microphone.

5.1.7.7 Input tab

The input tab lists input settings you have specified for a BioStation T2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.



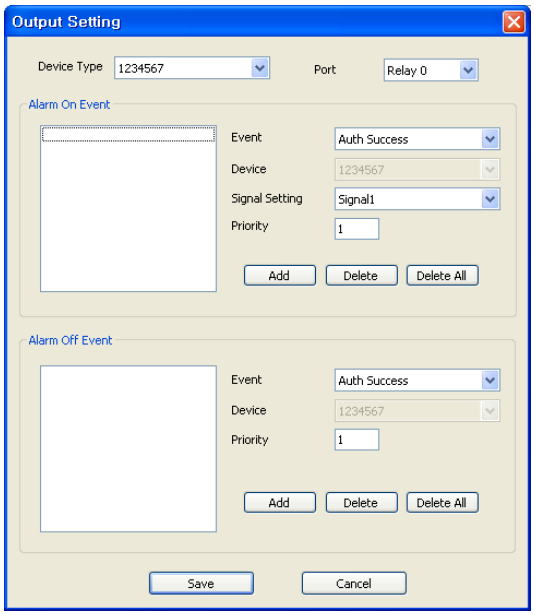
- **Device**: Select the BioStation T2 device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input**: The input port will be monitored for a triggering action (events specified with "Detect Input 0-3" in the **Output Setting** dialog box —see section 5.1.1.6).
  - **Emergency Open**: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms**: Cancel alarms associated with this device.

  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

- **Schedule**: Set the schedule during which the inputs will be monitored (*Always or No Time*).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.7.8 Output tab

The Output tab lists output settings you have specified for a BioStation T2 device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.



- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: Select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.

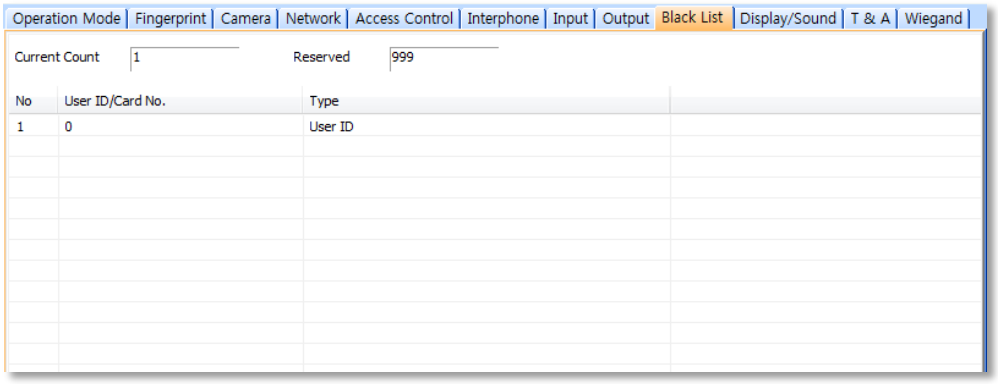
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Auth Duress*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.

Priority: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 "alarm on" event (activate) can be overridden only by an "alarm off" (deactivate) event with a priority of 1 or 2.

5.1.7.9 Black List tab

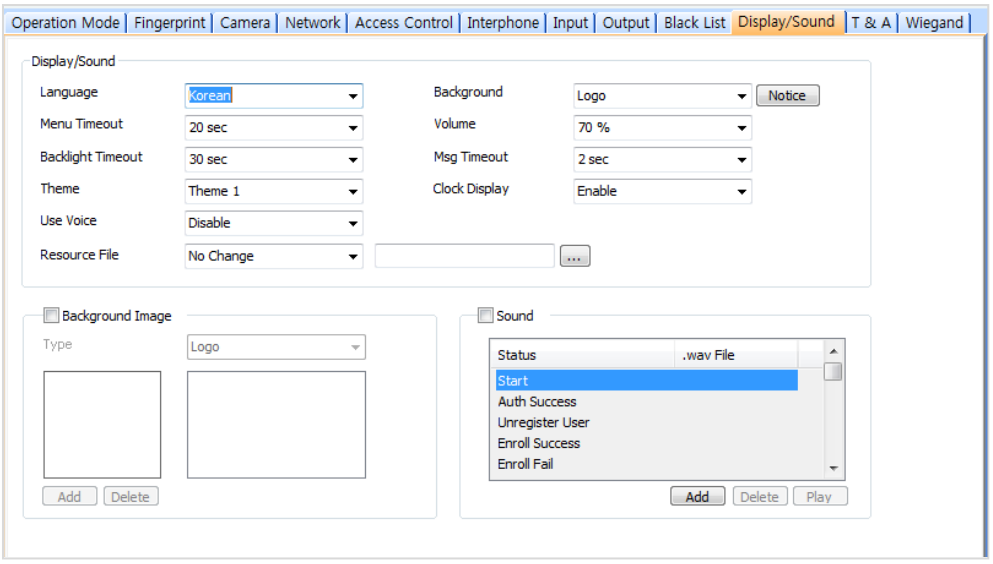
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of the user IDs and access cards that have been registered.
- **Reserved** : The remaining number of user IDs and access cards to be registered.

5.1.7.10 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation T2 display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

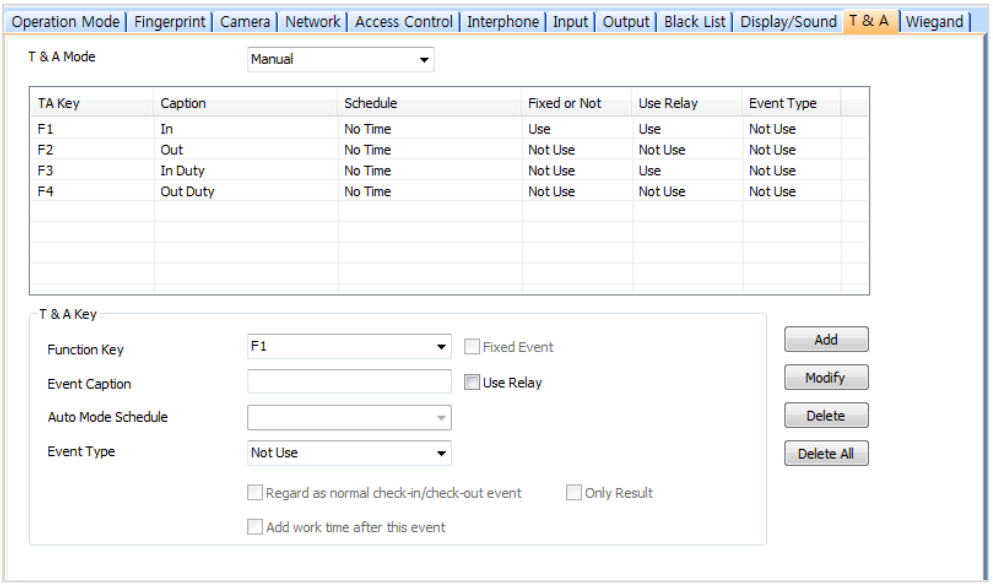


- **Display/Sound**
  - **Language**: Set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen.
  - **Backlight Timeout**: Set the length of time before the display goes dim.
  - **Theme**: set a display theme.
  - **Use Voice**: Set the device to notify you with voice messages (*Disable* or *Enable*).
  - **Resource File**: Set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the BioStation T2 display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
  - **Volume**: Set the volume of the BioStation device (*0%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed.
  - **Clock Display**: Set to display the current time on the device (Enable or Disable).

- **Background Image**: Click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.
  - **Type**: Set the type of background for the BioStation display (*Logo or Notice*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels for Notices and 480x800 pixels for Logos. Only one image at a time can be used as a logo or notice.
- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.7.11 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation T2 device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

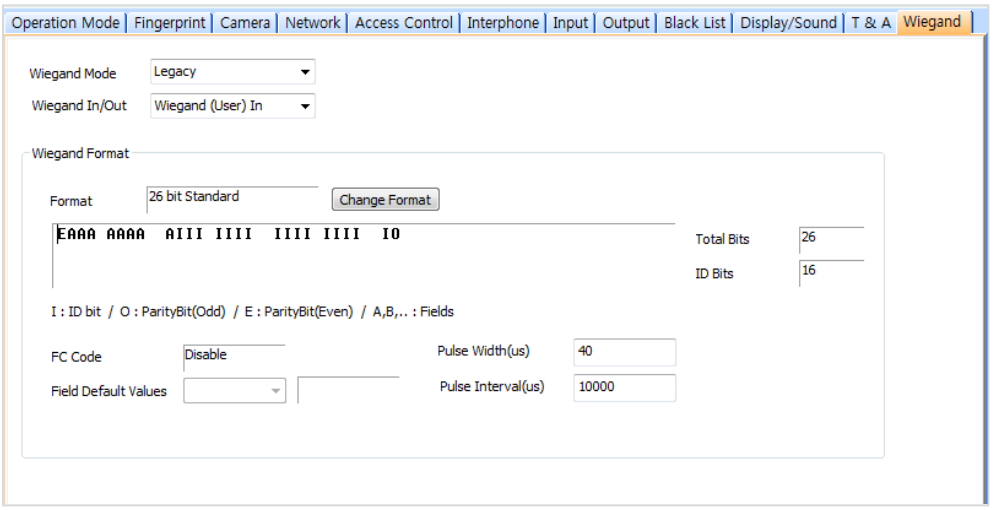


- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:

- **Function Key**: Select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
- **Event Caption**: Enter a caption for the event.
- **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
- **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.7.12 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation T2 device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.16.



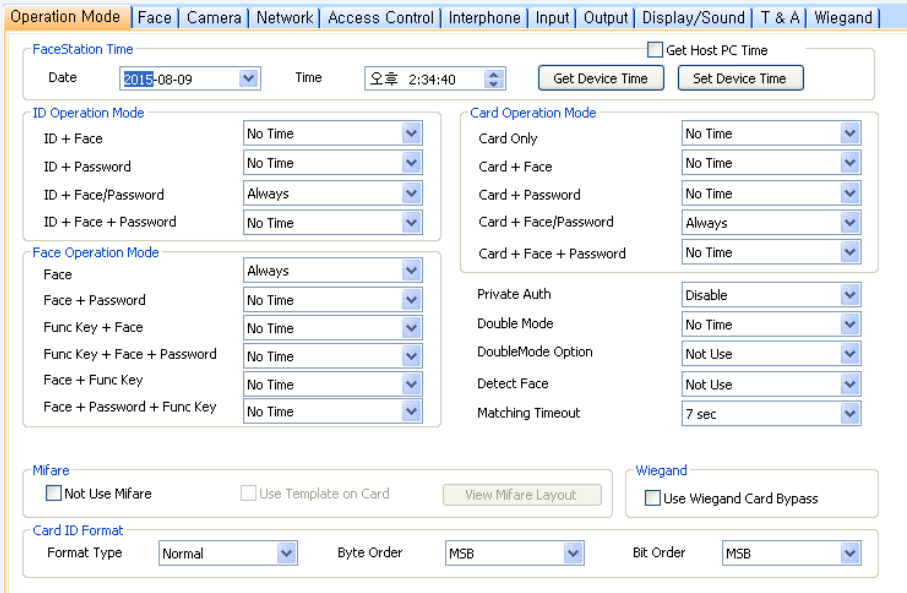
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the Wiegand input or output:
  - **Wiegand (User) In**: The ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.
  - **Wiegand (User) Out**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.
  - **Wiegand (Card) Out**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.1.8 Customize Settings for FaceStation Devices

The sections below describe the settings available for FaceStation devices. Customize the way FaceStation devices function by changing these settings to suit your particular environment and operational needs.

5.1.8.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for FaceStation devices.



- **FaceStation Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time:** Manually set the device time.
  - **Get Host PC Time**: Check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **ID Operation Mode**: The drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID + Face**: Set the device to require ID plus face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
  - **ID + Password**: Set the device to require ID plus password authorization (*Always*, *New Time Zone*, or *No Time*).
  - **ID + Face/Password**: Set the device to require ID plus face recognition or password authorization (*Always*, *New Time Zone*, or *No Time*).
  - **ID + Face + Password**: Set the device to require ID plus face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).

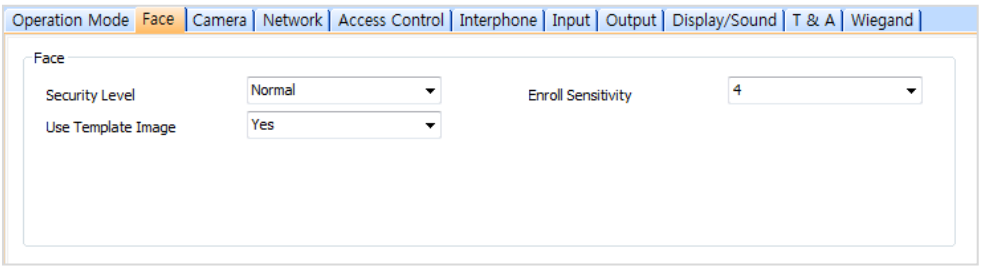
- **Card Operation Mode**
  - **Card Only**: Set the device to require only card authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Card + Face**: Set the device to require card plus face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Card + Password**: Set the device to require card plus password authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Card + Face/Password**: Set the device to require card plus face recognition or password authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Card + Face + Password**: Set the device to require card plus face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).
- **Face Operation Mode**
  - **Face**: Set the device to require only face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Face + Password**: Set the device to require face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Func Key + Face**: Set the device to require function key plus face recognition for authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Func Key + Face + Password**: Set the device to require function key plus face recognition plus password authorization (*Always*, *New Time Zone*, or *No Time*).
  - **Face + Func Key**: Set the device to require face recognition plus function key authorization, and then immediately proceed to T&A functions (*Always*, *New Time Zone*, or *No Time*).
  - **Face + Password + Func Key**: Set the device to require face recognition plus password plus function key authorization, and then immediately proceed to T&A functions (*Always*, *New Time Zone*, or *No Time*).
- **Other Options**
  - **Private Auth**: Set the device to allow a private authorization method (*Disable* or *Enable*). If enabled, the authentication mode of the user will be determined by a user's "Authorization" setting, which is located on the Details tab. If disabled, the authentication mode will be determined by operation mode settings of the device.
  - **Double Mode**: Set the device to require authentication of two users' IDs, access cards or face recognitions (*Always*, *New Time Zone*, or *No Time*). The timeout for presenting the second authentication is 15 seconds.
  - **Detect Face**: Set the device to capture a face image (*Use* or *Not Use*). Upon successful authentication, the captured image is stored in the event log.

  - **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).

- **Mifare**
  - **Not Use Mifare**: Check this box to disable MIFARE card authorization.
  - **Use Template on Card**: Not available with FaceSation devices.
  - **View Mifare Layout**: Not available with FaceSation devices.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).
  - **Bit Order:** Specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) or least significant bit (*LSB*).

5.1.8.2 Face tab

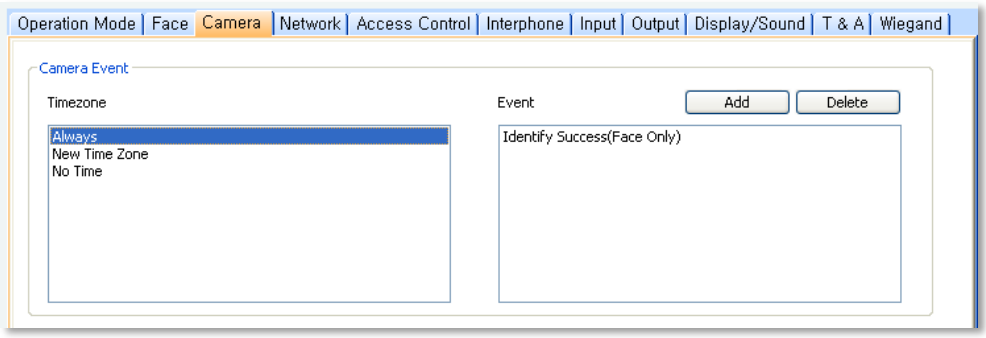
The Face tab allows you to customize face recognition settings for FaceStation devices.



- **Security Level**: Set the security level to use for face recognition (*Normal, Secure, or Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
- **Enroll Sensitivity**: Set the sensitivity of the face recognition system (*0 [Min]* to *9 [Max]*). A higher sensitivity setting will result in easier face recognition, but also increases the sensitivity to external visual noise.
- **Use Templete Image**: Set whether or not to display user face template images in the FaceStation device.

5.1.8.3 Camera tab

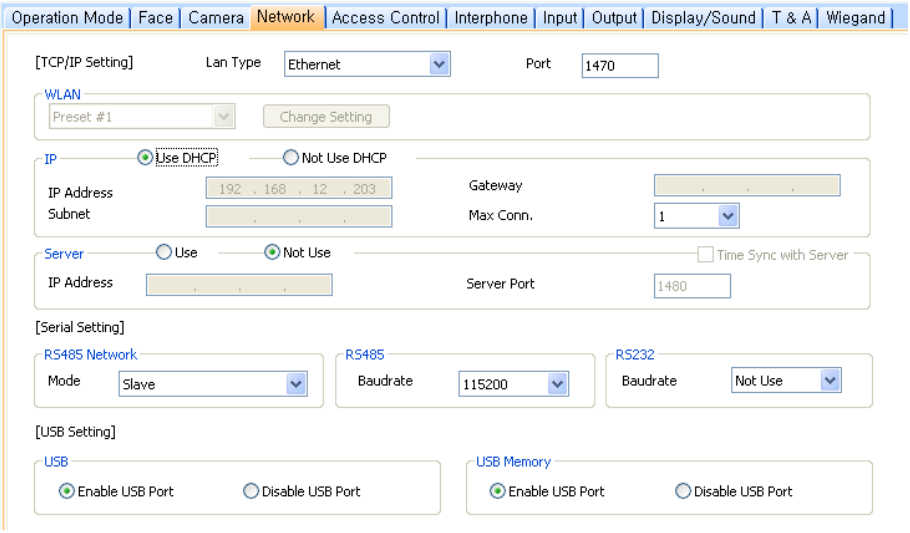
The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



Attention: We recommend that add the authentication events to the camera event for security. Add only a maximum of 30 events to reduce the network load between the device and the server.

5.1.8.4 Network tab

The Network tab allows you to customize network and server settings for FaceStation devices.

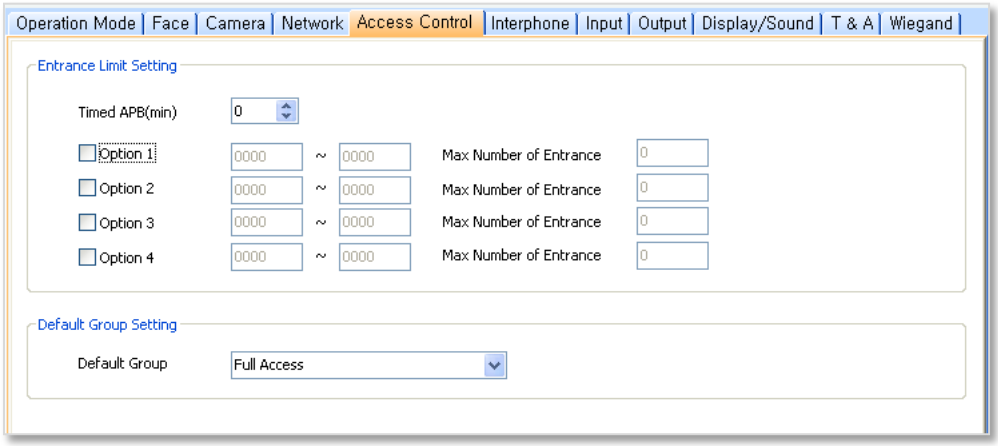


- **TCP/IP Setting**
  - **LAN Type**: Select a type of LAN connection from the drop-down list (*Disable*, *Ethernet*, or *Wireless LAN*).
  - **Port**: Specify a port to use for the device.
- **WLAN**
  - **Change Setting**: Click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, please see section 3.2.4.
- **IP**

  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet**: Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
  - **Max Conn.**: Specify the maximum number of connections to allow.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port**: Specify the port used to connect to the server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Disable*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
- **RS485**
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).
- **RS232**
  - **Baudrate**: Set the baud rate for a device connected via RS232 (*9600* to *115200*).
- **USB**: Click the option buttons to enable or disable the USB port on the FaceStation device.
- **USB Memory**: Click the option buttons to enable or disable the USB memory on the FaceStation device.

5.1.8.5 Access Control tab

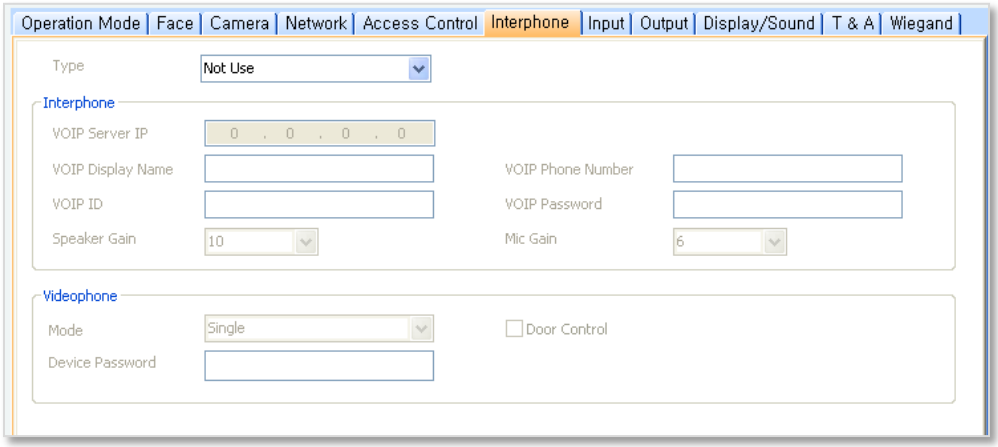
The Access Control tab allows you to customize entrance limit settings and default access groups for a FaceStation device.



- **Entrance Limit Setting**
  - **Timed APB (min)**: Set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's ID, access card, or fingerprint authorization for the time period specified here.
  - **Option 1-4**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
  - **Max Number of Entrance**: Set the maximum number of entries allowed during the specified time limit.
- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.8.6 Interphone tab

The Interphone tab allows you to set the device to act as an interphone to allow communication between people on either side of the door.



- **Type**: Select one of the following options:
  - **Analogue Interphone**: Choose this option to enable the analogue interphone.
  - **IP Interphone**: Choose this option to enable the VoIP feature. A telephone is required.
  - **BioStar Videophone**: Choose this option to enable the videophone feature that supports both video and voice calls. The supplied PC software is required. The BioStar videophone works only with the device firmware version of FaceStation V1.0 or later.

When you select **IP Interphone** in the Type drop-down list, specify the following settings:

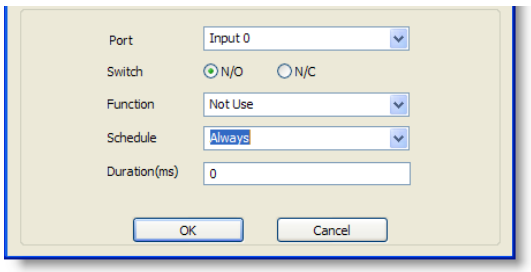
- **VOIP Server IP**: Specify an IP address for VOIP server.
- **VoIP Display Name**: Specify a name to use for communication through the interphone.
- **VoIP Phone Number**: Specify a phone number for the interphone.
- **VoIP ID**: Specify a user name to access the VoIP server.
- **VoIP Password**: Specify a password to access the VoIP server.
- **Speaker Gain**: Specify the volume of the speaker.
- **Mic Gain**: Specify the volume of the microphone.

When you select **Videophone** in the Type drop-down list, specify the following settings:

- **Mode**: Specify the videophone purpose (*Single* or *Extension*).
- **Door Control**: Check this option if the videophone is used for door access.
- **Device Password**: Enter the videophone device password.

5.1.8.7 Input tab

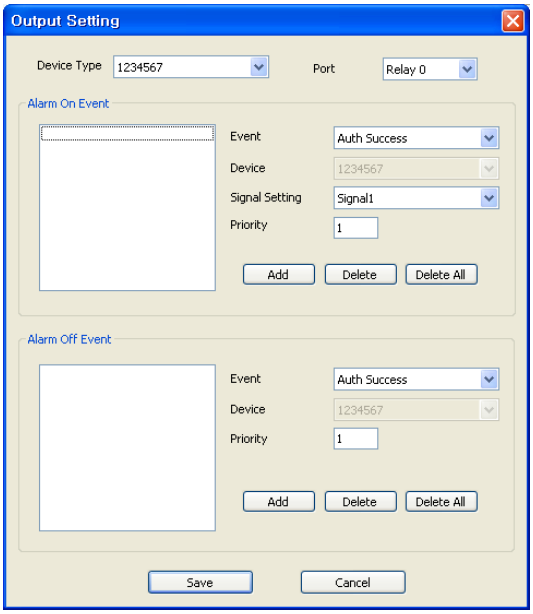
The input tab lists input settings you have specified for a FaceStation device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.



- **Device**: Select the FaceStation device for which you will add or modify settings.
- **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
- **Function**: Select an action to associate with the input:
  - **Not Use**: The input port will not be monitored.
  - **Generic Input**: The input port will be monitored for a triggering action (events specified with "Detect Input 0-3" in the **Output Setting** dialog box —see section 5.1.1.6).
  - **Emergency Open**: Open doors controlled by this device. The normal door open period will be ignored and doors will remain open until an operator sends a "Close Door" command via the Door/Zone Monitoring tab (see section 4.4.1).
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process face or card inputs. To enable communication again, an administrator must provide authentication at the device.
- **Schedule**: Set the schedule during which the inputs will be monitored (*Always or No Time*).
- **Duration (ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.

5.1.8.8 Output tab

The Output tab lists output settings you have specified for a FaceStation device. Buttons at the bottom of the tab allow you to add, modify, or delete output settings. To add or modify settings, you must specify them from the **Output Setting** dialog box. For more information about configuring output settings, see section 3.10.3.1.

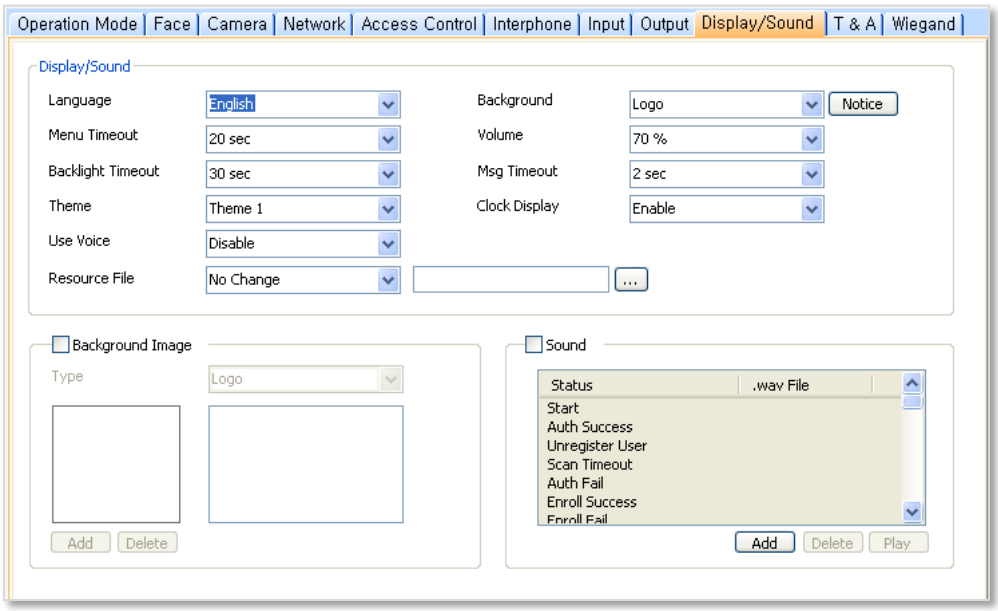


- **Device Type**: Select the device type for which you will add or modify settings.
- **Port**: select an output port (*Relay 0*). For Secure I/O devices, these settings are available: *Relay 0* or *Relay 1*.
- **Alarm On Event**: Specify settings and click **Add** to add the event to the Alarm On Event list. These events will activate an alarm.
  - **Event**: Select an event that will activate an alarm (*Auth Success*, *Auth Fail*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
  - **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, an alarm on (activate) event with a priority of 2 can be canceled only by an alarm off (deactivate) event with a priority of 1 or 2.

- **Alarm Off Event**: Specify settings and click **Add** to add the event to the Alarm Off Event list. These events will deactivate an alarm.
  - **Event**: Select an event that will deactivate an alarm (*Auth Success*, *Auth Fail*, *Anti-passback Fail*, *Access Not Granted*, *Entrance Limited*, *Admin Auth Success*, *Tamper On*, *Door Opened*, *Door Close*, *Forced Open Door*, *Held Open Door*, or *Detect Input #1-3*).
  - **Device**: Select the device to monitor for an alarm event.
- **Priority**: Set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, a priority 2 “alarm on” event (activate) can be overridden only by an “alarm off" (deactivate) event with a priority of 1 or 2.

5.1.8.9 Display/Sound tab

The Display/Sound tab allows you to customize the FaceStation display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



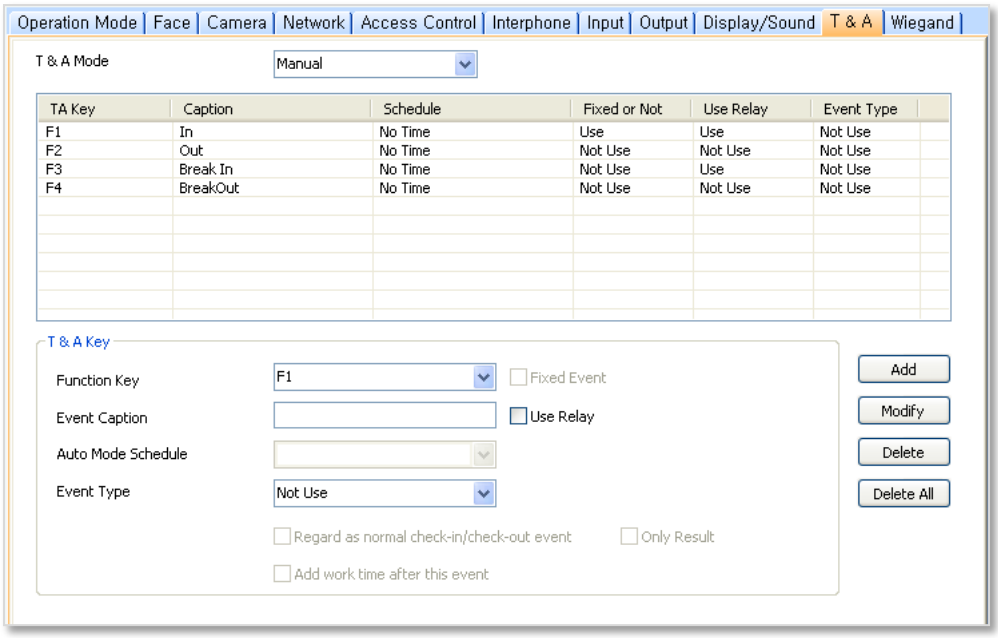
- **Display/Sound**
  - **Language**: Set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen (*Infinite*, *10 sec*, *20 sec*, or *30 sec*).
  - **Backlight Timeout**: Set the length of time before the display goes dim (*Infinite*, *10 sec*, *20 sec*, *30 sec*, *40 sec*, *50 sec*, or *60 sec*).
  - **Theme**: set a display theme (*Theme 1-4*)
  - **Use Voice**: Set the device to notify you with voice messages (*Disable* or *Enable*).

  - **Resource File**: Set the language resource file to use for the BioStar interface (*No Change*, *Korean*, *English*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the FaceStation display (*Logo*, *Notice*, *Slide Show,* or *PDF*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels each. Only one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.
  - **Volume**: Set the volume of the FaceStation device (*0%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed (*0.5-5 sec*).
  - **Clock Display**: Set to display the current time on the device (Enable or Disable).

- **Background Image**: Click this checkbox to upload new background images. Click the plus sign (+) to locate and add a new image file.
  - **Type**: Set the type of background for the FaceStation display (*Logo*, *Notice*, *Slide Show,* or *PDF*). Supported file types (JPG, GIF, BMP, PNG and PDF) cannot exceed 480x800 pixels for Notices and 480x800 pixels for Logos. Only one image at a time can be used as a logo or notice.
- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.8.10 T&A tab

The T&A tab allows you to configure the mode and key settings for a FaceStation device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

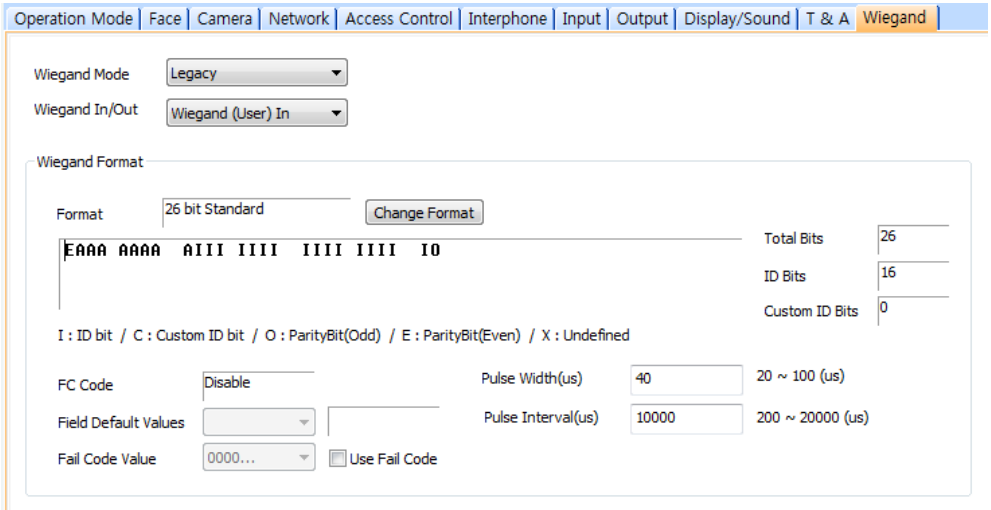


- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key**: Select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption**: Enter a caption for the event.
  - **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, see section 3.7.1.

- **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.8.11 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a FaceStation device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.16.



- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the Wiegand input or output:
  - **Wiegand (User) In**: The ID field of the Wiegand string is interpreted as a user ID.
  - **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.

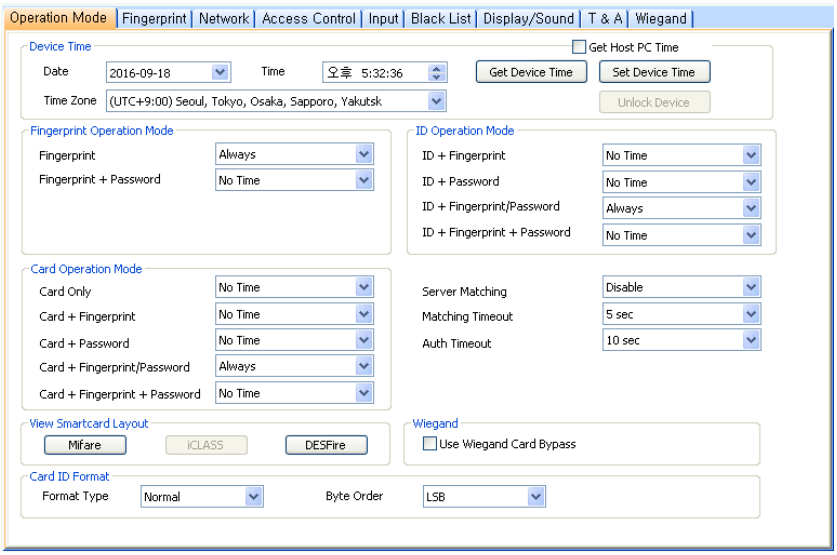
- **Wiegand (User) Out**: Inserts the user ID of the authenticated user in the ID field of the Wiegand string.
- **Wiegand (Card) Out**: Inserts the card ID of the authenticated user in the ID field of the Wiegand string.

5.1.9 Customize Settings for BioStation 2 Devices

The sections below describe the settings available for BioStation 2 devices. Customize the way BioStation 2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.9.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation 2 devices.



- **Device Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time**: Manually set the device time.
  - **Time Zone**: Select the time zone you wish to use.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **Fingerprint Operation Mode**
  - **Fingerprint**: Set the device to require only fingerprint authorization (*Always*, or *No Time*).

  - **Fingerprint + Password**: Set the device to require fingerprint plus password authorization (*Always*, or *No Time*).

- **ID Operation Mode**: The drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID + Fingerprint**: Set the device to require ID plus fingerprint authorization (*Always*, or *No Time*).
  - **ID + Password**: Set the device to require ID plus password authorization (*Always*, or *No Time*).
  - **ID + Fingerprint/Password**: Set the device to require ID plus fingerprint or password authorization (*Always*, or *No Time*).
  - **ID + Fingerprint + Password**: Set the device to require ID plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Card Operation Mode**
  - **Card Only**: Set the device to require only card authorization (*Always*, or *No Time*).
  - **Card + Fingerprint**: Set the device to require card plus fingerprint authorization (*Always*, or *No Time*).
  - **Card + Password**: Set the device to require card plus password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint/Password**: Set the device to require card plus fingerprint or password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint + Password**: Set the device to require card plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Other Options**
  - **Server Matching**: Enable this setting to perform user ID, fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the user ID, fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).
  - **Auth Timeout**: Sets the standby time (3 seconds – 20 seconds) for authenticating the next credential when two or more credentials are used.
- **View Smartcard Layout**

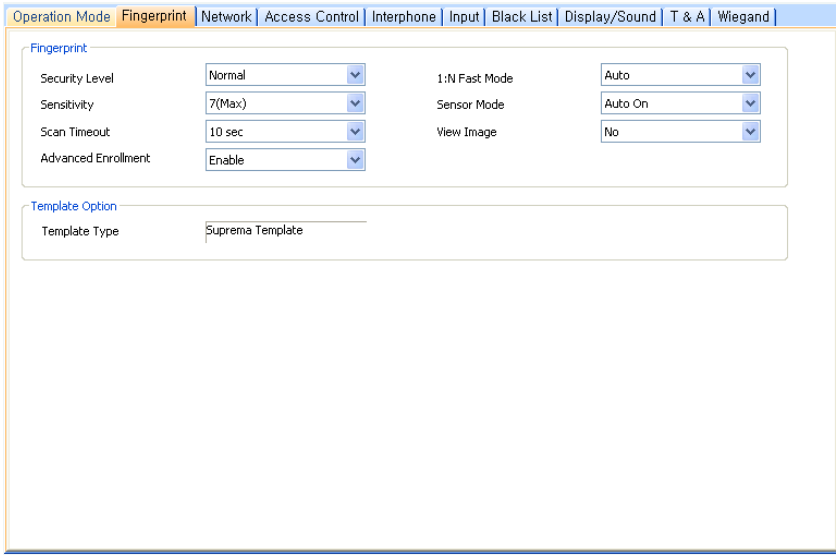
- **MIFARE**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **iCLASS**: Click this button to view the iCLASS layout used by the device. For more information about configuring iCLASS layouts, please see section 3.6.4.9.
- **DESFire**: Click this button to view the DESFire layout used by the device. For more information about configuring DESFire layouts, please see section 3.6.4.8.

- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).

  Note: The device versions 1.x and 2.x have different methods to read card data, but BioStar corrects card data, so card data can be used in the same way. Therefore, MSB/LSB should be set in the same way in the device versions 1.x and 2.x. The card ID displayed by the device may be shown as horizontally reversed, since it is displayed based on Hexa value, but this can be ignored because card data can nevertheless be read correctly.
  - In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.
  - **Use Wiegand Card Bypass**: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

5.1.9.2 Fingerprint tab

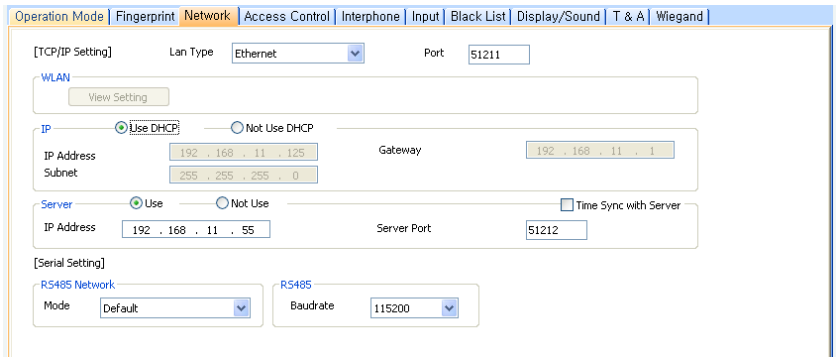
The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation 2 devices.



- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Sensitivity**: Set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **Scan Timeout**: Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Advanced Enrollment**: Checks the quality of the scanned fingerprint to avoid the poor quality fingerprint template enrollment. The user will be alerted when the quality of the fingerprint scanned is low and given enrollment instructions.
  - **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **Sensor Mode**: If the option is set to **Auto On**, the sensor will automatically go on when it detects a finger. If the option is set to **Always On**, the sensor will always be on.
  - **View Image**: Set to show or hide fingerprint images on the BioStation 2 display (*Yes* or *No*).
  - **Template Option**: Displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

5.1.9.3 Network tab

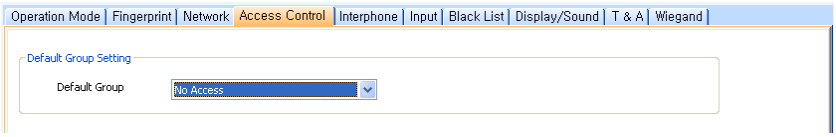
The Network tab allows you to customize network and server settings for BioStation 2 devices.



- **TCP/IP Setting**
  - **LAN Type**: Select a type of LAN connection from the drop-down list (*Ethernet*, or *Wireless LAN*).
  - **Port**: Specify a port to use for the device.
- **WLAN**
  - **Change Setting**: Click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.
- **IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet:** Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port:** Specify the port used to connect to the server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Default*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.9.4 Access Control tab

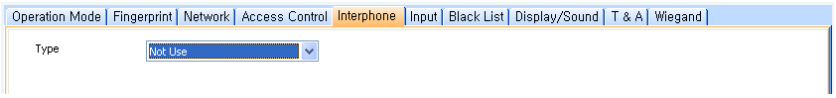
The Access Control tab allows you to customize default access groups for a BioStation 2 device.



- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.9.5 Interphone tab

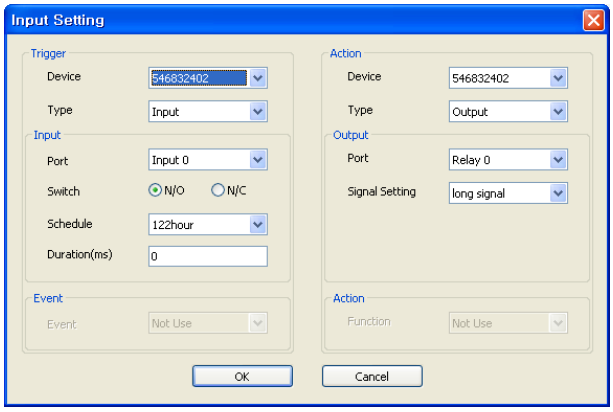
The Interphone tab allows you to set the device to act as an interphone to allow communication between people on either side of the door.



- **Type**
  - **Analogue Interphone**: Choose this option to enable the analogue interphone.

5.1.9.6 Input tab

The input tab lists input settings you have specified for a BioStation 2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.

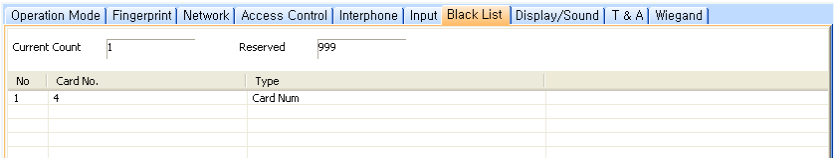


- **Trigger**
  - **Device**: Select a device which a specific event will be monitored.
  - **Type**: Select **Input** or **Event**.
- **Input**: If the **Type** of **Trigger** is set to **Input**, can be set.

  - **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*).
  - **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
  - **Schedule**: Set the schedule during which the inputs will be monitored (*Always or No Time*).
  - **Duration(ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.
- **Event**: Set the trigger event. If the **Type** of **Trigger** is set to **Event**, can be set.
- **Action**
  - **Device**: Select a device which performs the action.
  - **Type**: Select **Output** or **Function**.
- **Output**: If the **Type** of **Action** is set to **Output**, can be set.
  - **Port**: Select an output port.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Function**: Select an action to associate with the input. If the **Type** of **Action** is set to **Function**, can be set.:
  - **Not Use**: The input port will not be monitored.
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

5.1.9.7 Black List tab

The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.

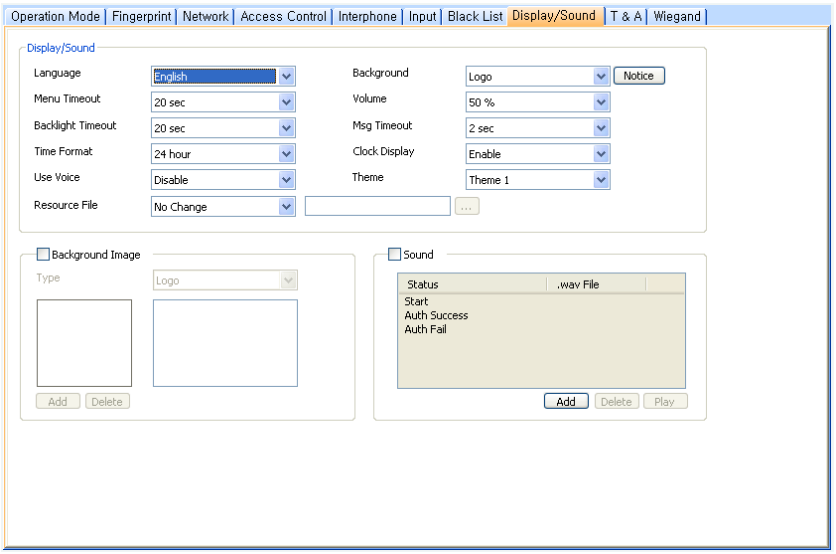


- **Current Count**: The total number of the user IDs and access cards that have been registered.
- **Reserved** : The remaining number of user IDs and access cards to be registered.

5.1.9.8 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation 2 display and event sounds. To save changes to display or sound settings, you must click **Apply**

at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

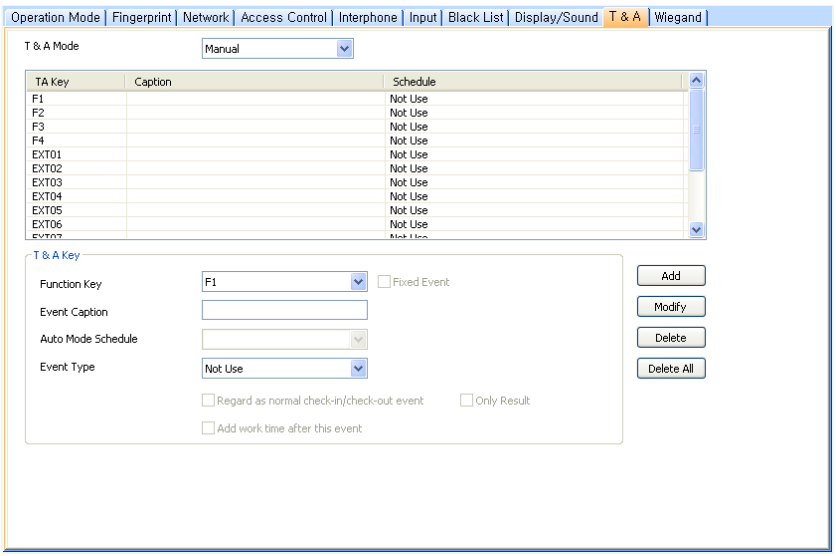


- **Display/Sound**
  - **Language**: Set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen.
  - **Backlight Timeout**: Set the length of time before the display goes dim.
  - **Theme**: set a display theme.
  - **Use Voice**: Set the device to notify you with voice messages **(***Disable* or *Enable***).**
  - **Resource File**: Set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the BioStation 2 display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 320x240 pixels each.
  - **Notice**: Click this button to create a notice that will be shown on the BioStation 2 display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
  - **Volume**: Set the volume of the BioStation 2 device (*0%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed.
  - **Clock Display**: Set to display the current time on the device (Enable or Disable).
- **Background Image**: Click this checkbox to upload new background images. Click **Add** to locate and add a new image file.

- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.9.9 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation 2 device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



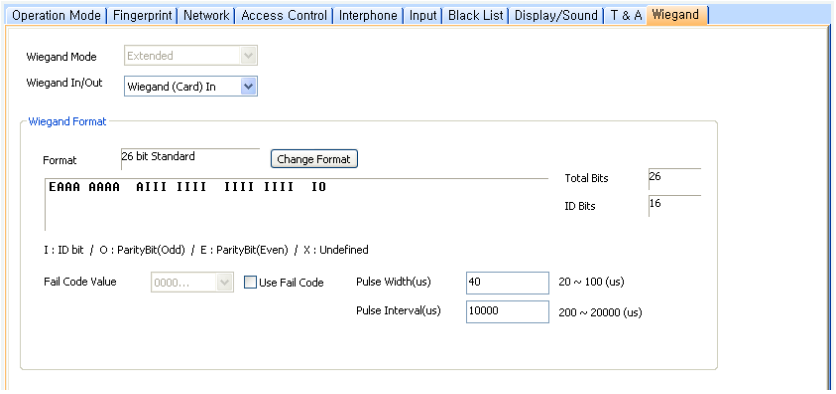
- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key**: Select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption**: Enter a caption for the event.
  - **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-

down list. For more information on creating a timezone, please see section 3.7.1.

– **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.9.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation 2 device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.13.



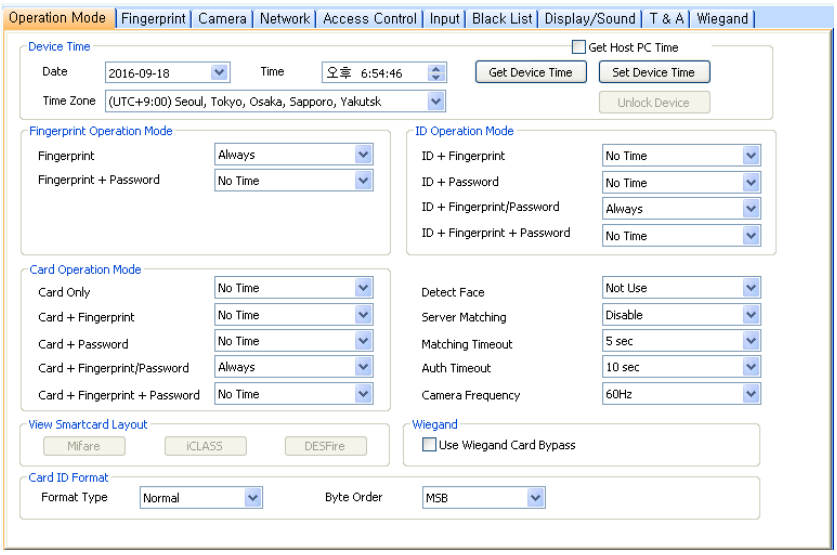
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Extended*). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the Wiegand input or output:
  – **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.

5.1.10 Customize Settings for BioStation A2 Devices

The sections below describe the settings available for BioStation A2 devices. Customize the way BioStation A2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.10.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation A2 devices.



- **Device Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time**: Manually set the device time.
  - **Time Zone**: Select the time zone you wish to use.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **Fingerprint Operation Mode**
  - **Fingerprint**: Set the device to require only fingerprint authorization (*Always*, or *No Time*).
  - **Fingerprint + Password**: Set the device to require fingerprint plus password authorization (*Always*, or *No Time*).
- **ID Operation Mode**: The drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify

authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.

- **ID + Fingerprint**: Set the device to require ID plus fingerprint authorization (*Always*, or *No Time*).
- **ID + Password**: Set the device to require ID plus password authorization (*Always*, or *No Time*).
- **ID + Fingerprint/Password**: Set the device to require ID plus fingerprint or password authorization (*Always*, or *No Time*).
- **ID + Fingerprint + Password**: Set the device to require ID plus fingerprint plus password authorization (*Always*, *or No Time*).

- **Card Operation Mode**
  - **Card Only**: Set the device to require only card authorization (*Always*, or *No Time*).
  - **Card + Fingerprint**: Set the device to require card plus fingerprint authorization (*Always*, or *No Time*).
  - **Card + Password**: Set the device to require card plus password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint/Password**: Set the device to require card plus fingerprint or password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint + Password**: Set the device to require card plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Other Options**
  - **Detect Face**: Set the device to capture a face image. Upon successful authentication, the captured image is stored in the event log.
  - **Server Matching**: Enable this setting to perform user ID, fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the user ID, fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).
  - **Auth Timeout**: Sets the standby time (3 seconds – 20 seconds) for authenticating the next credential when two or more credentials are used.
  - **Camera Frequency**: Sets the camera frequency. If you set the frequency incorrectly in an environment in which fluorescent light is used, flickering on the image may occur. Contract a local distributor for making inquiries. (**50 Hz**, **60 Hz**)
- **View Smartcard Layout**

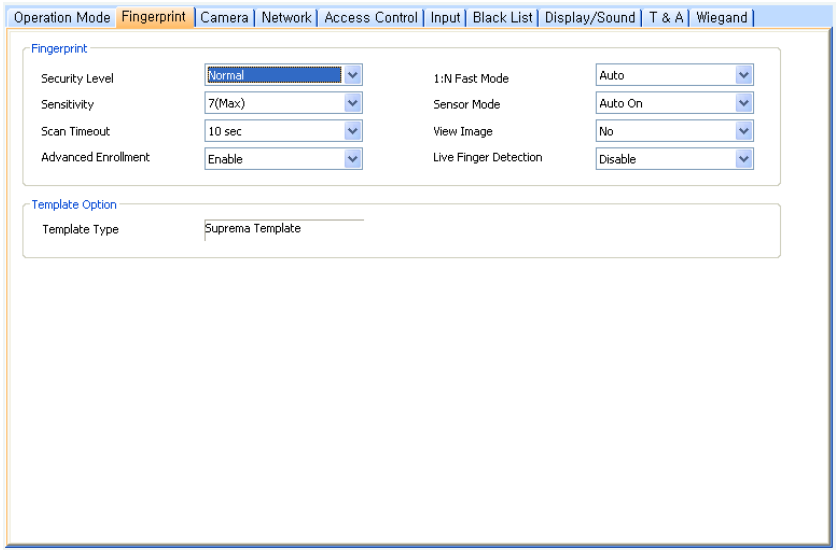
- **MIFARE**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
- **iCLASS**: Click this button to view the iCLASS layout used by the device. For more information about configuring iCLASS layouts, please see section 3.6.4.9.
- **DESFire**: Click this button to view the DESFire layout used by the device. For more information about configuring DESFire layouts, please see section 3.6.4.8.

- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).

  Note: The device versions 1.x and 2.x have different methods to read card data, but BioStar corrects card data, so card data can be used in the same way. Therefore, MSB/LSB should be set in the same way in the device versions 1.x and 2.x. The card ID displayed by the device may be shown as horizontally reversed, since it is displayed based on Hexa value, but this can be ignored because card data can nevertheless be read correctly.
  - In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.
  - **Use Wiegand Card Bypass**: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

5.1.10.2 Fingerprint tab

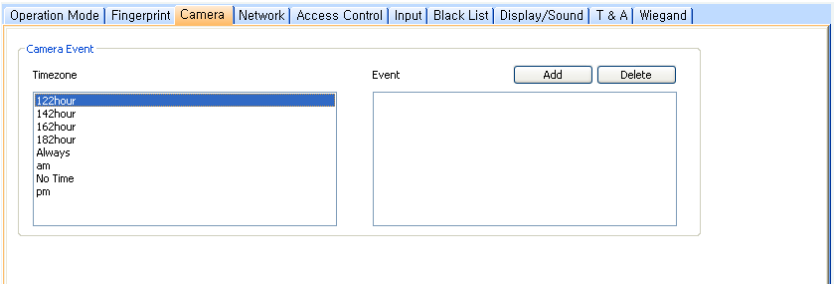
The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation A2 devices.



- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Sensitivity**: Set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **Scan Timeout**: Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Advanced Enrollment**: Checks the quality of the scanned fingerprint to avoid the poor quality fingerprint template enrollment. The user will be alerted when the quality of the fingerprint scanned is low and given enrollment instructions.
  - **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
  - **Sensor Mode**: If the option is set to **Auto On**, the sensor will automatically go on when it detects a finger. If the option is set to **Always On**, the sensor will always be on.
  - **View Image**: Set to show or hide fingerprint images on the BioStation A2 display (*Yes* or *No*).
  - **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.
  - **Template Option**: Displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

5.1.10.3 Camera tab

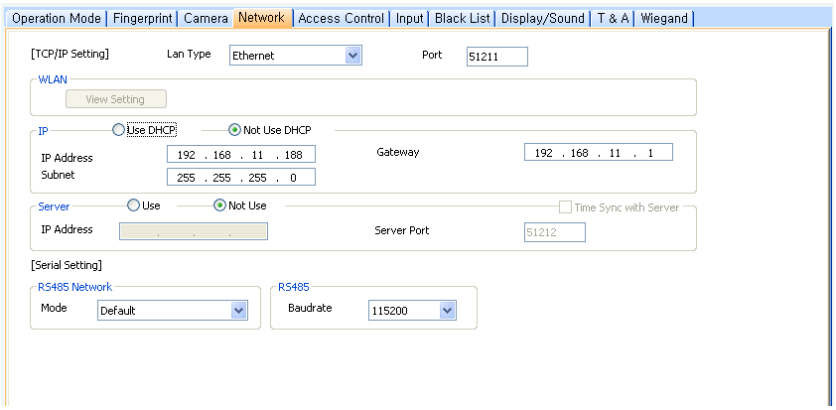
The Camera tab allows you to control how the camera is used for authorization purposes. In the Timezone field, select a timezone for the specified event. Click **Add** to select an event that will activate the camera. Click **Apply** to save your settings.



Attention: We recommend that add the authentication events to the camera event for security. Add only a maximum of 30 events to reduce the network load between the device and the server.

5.1.10.4 Network tab

The Network tab allows you to customize network and server settings for BioStation A2 devices.

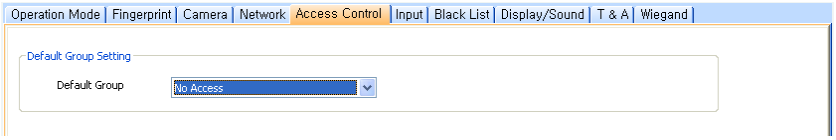


- **TCP/IP Setting**
  - **LAN Type**: Select a type of LAN connection from the drop-down list (*Ethernet*, or *Wireless LAN*).
  - **Port**: Specify a port to use for the device.
- **WLAN**
  - **Change Setting**: Click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.

- **IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet:** Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port:** Specify the port used to connect to the server.
  - **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.
- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Default*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.10.5 Access Control tab

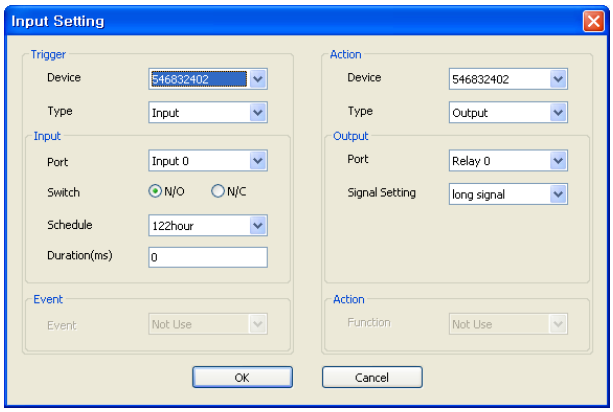
The Access Control tab allows you to customize default access groups for a BioStation A2 device.



- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.10.6 Input tab

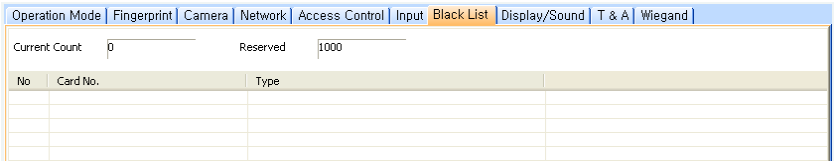
The input tab lists input settings you have specified for a BioStation A2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.



- **Trigger**
  - **Device**: Select a device which a specific event will be monitored.
  - **Type**: Select **Input** or **Event**.
- **Input**: If the **Type** of **Trigger** is set to **Input**, can be set.
  - **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*).
  - **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
  - **Schedule**: Set the schedule during which the inputs will be monitored (*Always or No Time*).
  - **Duration(ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.
- **Event**: Set the trigger event. If the **Type** of **Trigger** is set to **Event**, can be set.
- **Action**
  - **Device**: Select a device which performs the action.
  - **Type**: Select **Output** or **Function**.
- **Output**: If the **Type** of **Action** is set to **Output**, can be set.
  - **Port**: Select an output port.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Function**: Select an action to associate with the input. If the **Type** of **Action** is set to **Function**, can be set.:
  - **Not Use**: The input port will not be monitored.
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

5.1.10.7 Black List tab

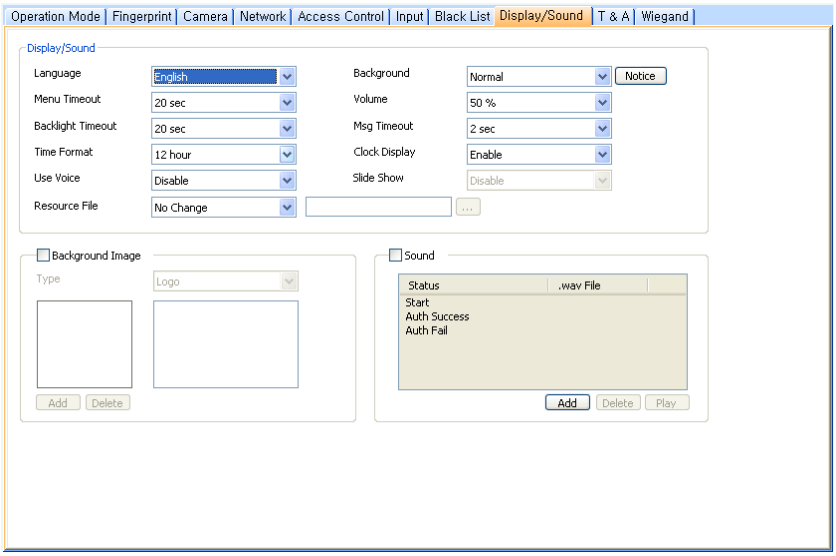
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of the user IDs and access cards that have been registered.
- **Reserved** : The remaining number of user IDs and access cards to be registered.

5.1.10.8 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation A2 display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



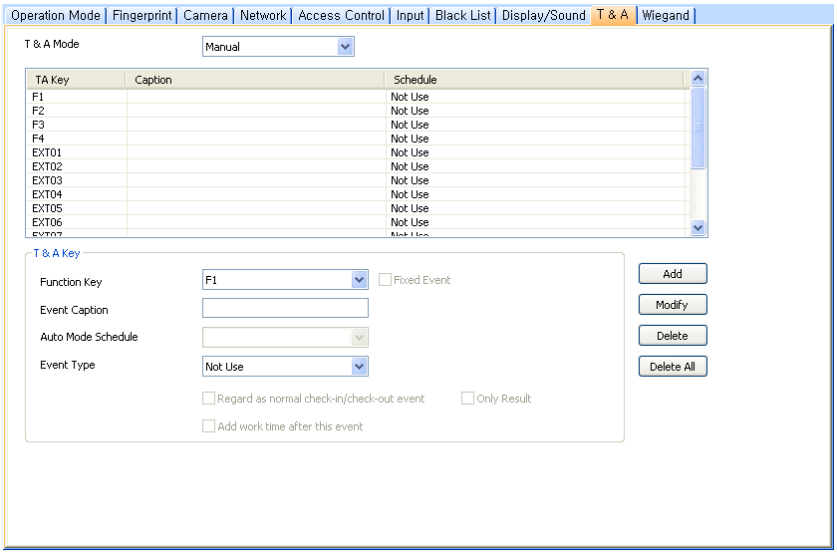
- **Display/Sound**
  - **Language**: Set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen.
  - **Backlight Timeout**: Set the length of time before the display goes dim.
  - **Theme**: set a display theme.
  - **Use Voice**: Set the device to notify you with voice messages (*Disable* or *Enable*).

  - **Resource File**: Set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the BioStation A2 display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP, and PNG) cannot exceed 480x854 pixels each.
  - **Notice**: Click this button to create a notice that will be shown on the BioStation A2 display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
  - **Volume**: Set the volume of the BioStation A2 device (*0%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed.
  - **Clock Display**: Set to display the current time on the device (Enable or Disable).

- **Background Image**: Click this checkbox to upload new background images. Click **Add** to locate and add a new image file.
- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.10.9 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation A2 device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

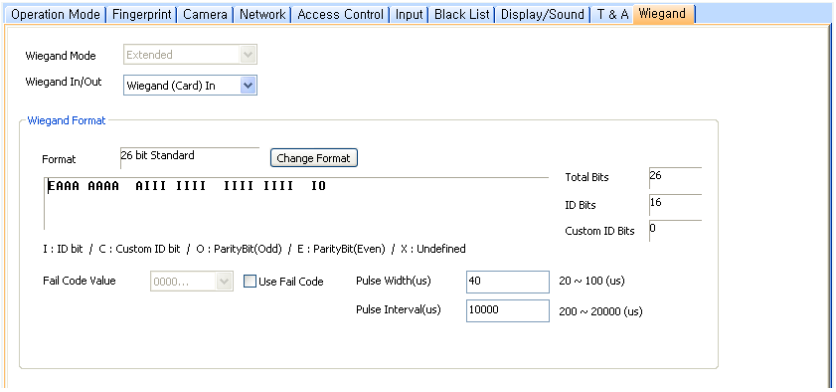


- **T&A Mode**: Set the time and attendance mode:

  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key**: Select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption**: Enter a caption for the event.
  - **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
  - **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the “Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the “Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the “Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.10.10 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation A2 device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.13.



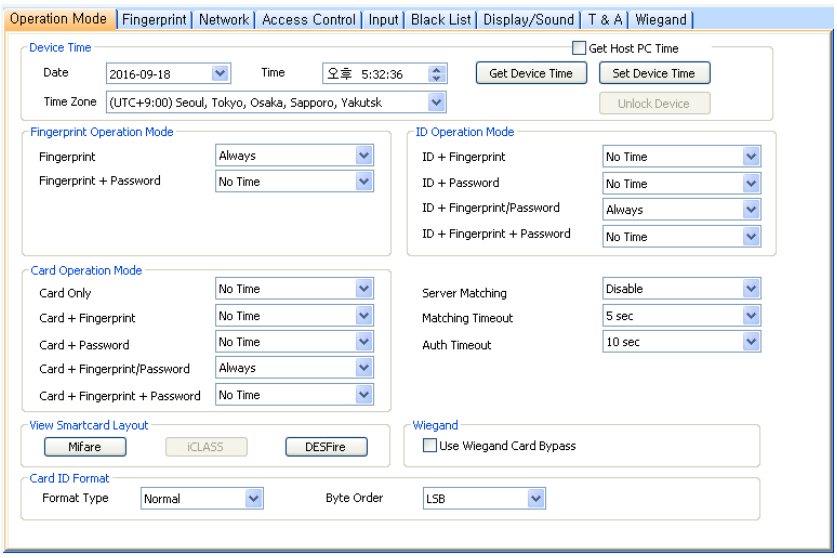
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Extended*). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the Wiegand input or output:
  - **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.

5.1.11 Customize Settings for BioStation L2 Devices

The sections below describe the settings available for BioStation L2 devices. Customize the way BioStation L2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.11.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation L2 devices.



- **Device Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time**: Manually set the device time.
  - **Time Zone**: Select the time zone you wish to use.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **Fingerprint Operation Mode**
  - **Fingerprint**: Set the device to require only fingerprint authorization (*Always*, or *No Time*).
  - **Fingerprint + Password**: Set the device to require fingerprint plus password authorization (*Always*, or *No Time*).
- **ID Operation Mode**: The drop-down lists in this area allow you to control the authentication mode by schedule. For example, you can choose a normal authentication mode for working hours and a more strict authentication mode for hours outside the normal schedule. You can specify authentication modes either by device or by user (see section 5.4.1). Unless a particular mode is specified for a user, the device authentication mode will apply.
  - **ID + Fingerprint**: Set the device to require ID plus fingerprint authorization (*Always*, or *No Time*).
  - **ID + Password**: Set the device to require ID plus password authorization (*Always*, or *No Time*).
  - **ID + Fingerprint/Password**: Set the device to require ID plus fingerprint or password authorization (*Always*, or *No Time*).
  - **ID + Fingerprint + Password**: Set the device to require ID plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Card Operation Mode**
  - **Card Only**: Set the device to require only card authorization (*Always*, or *No Time*).
  - **Card + Fingerprint**: Set the device to require card plus fingerprint authorization (*Always*, or *No Time*).
  - **Card + Password**: Set the device to require card plus password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint/Password**: Set the device to require card plus fingerprint or password authorization (*Always*, or *No Time*).
  - **Card + Fingerprint + Password**: Set the device to require card plus fingerprint plus password authorization (*Always*, *or No Time*).
- **Other Options**

- **Server Matching**: Enable this setting to perform user ID, fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the user ID, fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
- **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).
- **Auth Timeout**: Sets the standby time (3 seconds – 20 seconds) for authenticating the next credential when two or more credentials are used.

• **View Smartcard Layout**
  - **MIFARE**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
  - **iCLASS**: Click this button to view the iCLASS layout used by the device. For more information about configuring iCLASS layouts, please see section 3.6.4.9.
  - **DESFire**: Click this button to view the DESFire layout used by the device. For more information about configuring DESFire layouts, please see section 3.6.4.8.

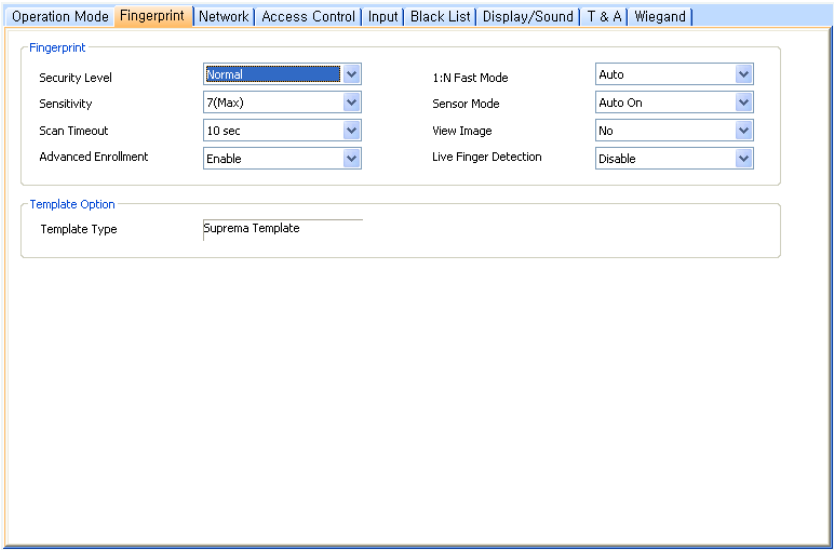
• **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).

  Note: The device versions 1.x and 2.x have different methods to read card data, but BioStar corrects card data, so card data can be used in the same way. Therefore, MSB/LSB should be set in the same way in the device versions 1.x and 2.x. The card ID displayed by the device may be shown as horizontally reversed, since it is displayed based on Hexa value, but this can be ignored because card data can nevertheless be read correctly.
  - In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.

– **Use Wiegand Card Bypass**: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

5.1.11.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for BioStation L2 devices.

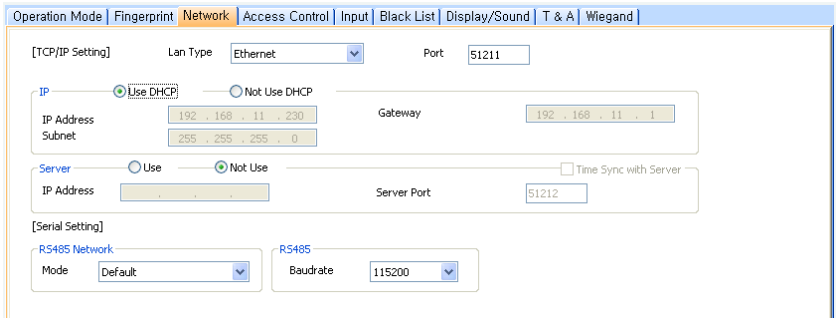


- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Sensitivity**: Set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **Scan Timeout**: Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Advanced Enrollment**: Checks the quality of the scanned fingerprint to avoid the poor quality fingerprint template enrollment. The user will be alerted when the quality of the fingerprint scanned is low and given enrollment instructions.
  - **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.

- **Sensor Mode**: If the option is set to **Auto On**, the sensor will automatically go on when it detects a finger. If the option is set to **Always On**, the sensor will always be on.
- **View Image**: Set to show or hide fingerprint images on the BioStation L2 display (*Yes* or *No*).
- **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.
- **Template Option**: Displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

5.1.11.3 Network tab

The Network tab allows you to customize network and server settings for BioStation L2 devices.



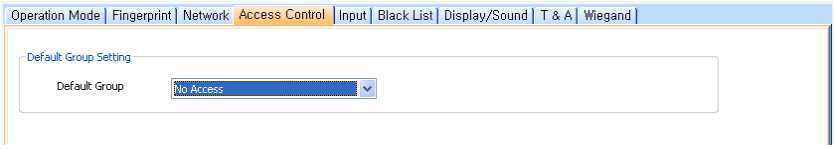
- **TCP/IP Setting**
  - **LAN Type**: Select a type of LAN connection from the drop-down list (*Ethernet*, or *Wireless LAN*).
  - **Port**: Specify a port to use for the device.
- **WLAN**
  - **Change Setting**: Click to specify settings for a wireless local area network (WLAN). This option is active only when WLAN is selected as the TCP/IP setting. For more information about configuring settings for a WLAN, see section 3.2.4.
- **IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet:** Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.

- **IP Address**: Specify an IP address for the BioStar server.
- **Server Port:** Specify the port used to connect to the server.
- **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.

- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Default*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.11.4 Access Control tab

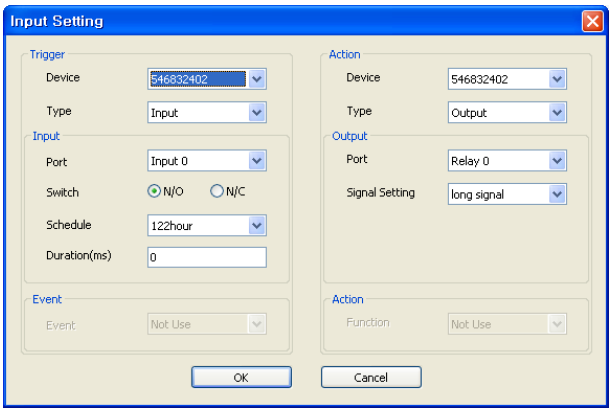
The Access Control tab allows you to customize default access groups for a BioStation L2 device.



- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.11.5 Input tab

The input tab lists input settings you have specified for a BioStation L2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.

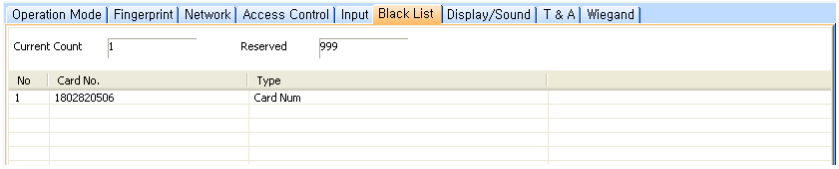


- **Trigger**
  - **Device**: Select a device which a specific event will be monitored.

  - **Type**: Select **Input** or **Event**.
- **Input**: If the **Type** of **Trigger** is set to **Input**, can be set.
  - **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*).
  - **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
  - **Schedule**: Set the schedule during which the inputs will be monitored (*Always or No Time*).
  - **Duration(ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.
- **Event**: Set the trigger event. If the **Type** of **Trigger** is set to **Event**, can be set.
- **Action**
  - **Device**: Select a device which performs the action.
  - **Type**: Select **Output** or **Function**.
- **Output**: If the **Type** of **Action** is set to **Output**, can be set.
  - **Port**: Select an output port.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Function**: Select an action to associate with the input. If the **Type** of **Action** is set to **Function**, can be set.:
  - **Not Use**: The input port will not be monitored.
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

5.1.11.6 Black List tab

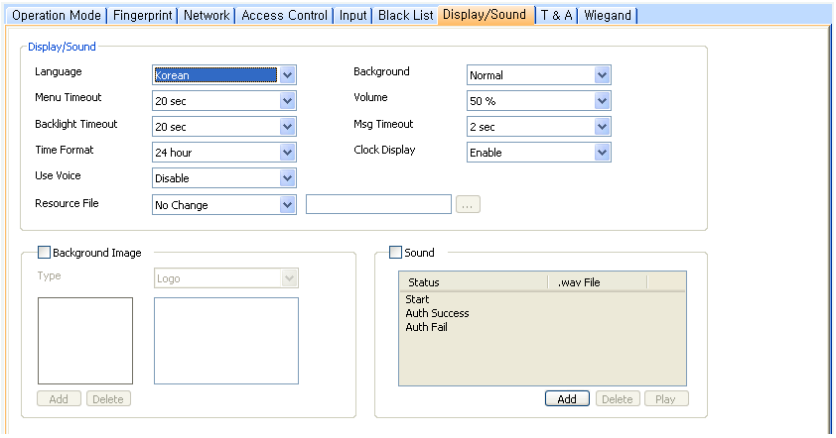
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of the user IDs and access cards that have been registered.
- **Reserved** : The remaining number of user IDs and access cards to be registered.

5.1.11.7 Display/Sound tab

The Display/Sound tab allows you to customize the BioStation L2 display and event sounds. To save changes to display or sound settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.

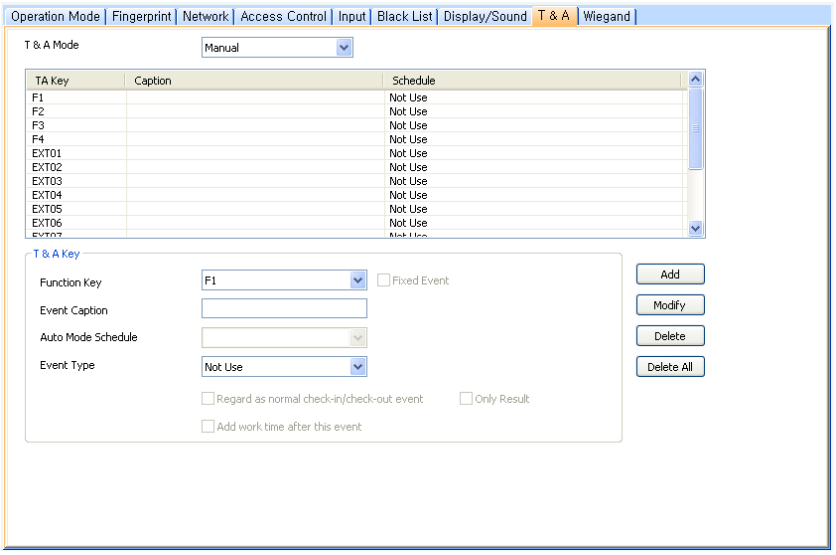


- **Display/Sound**
  - **Language**: Set the language to use on the display (*Korean*, *English*, or *Custom*).
  - **Menu Timeout**: Set the length of time before the display will return to the idle screen.
  - **Backlight Timeout**: Set the length of time before the display goes dim.
  - **Theme**: set a display theme.
  - **Use Voice**: Set the device to notify you with voice messages **(***Disable* or *Enable***).**
  - **Resource File**: Set the language resource file to use for the BioStar interface (*No Change*, *English*, *Korean*, or *Custom*). To use a language resource file other than English or Korean, select *Custom* and then click the ellipsis (…) button to locate the resource file.
  - **Background**: Set the type of background for the BioStation L2 display (*Logo*, *Notice*, or *Slide Show*). Supported file types (JPG, GIF, BMP and PNG) cannot exceed 220x176 pixels each.
  - **Notice**: Click this button to create a notice that will be shown on the BioStation L2 display. After creating a notice, you can click **Apply** to apply the notice to the current device or **Apply to Others** to apply the notice to additional devices.
  - **Volume**: Set the volume of the BioStation L2 device (*0%* to *100%*).
  - **Msg Timeout**: Set the length of time that a failure or confirmation message will be displayed.
  - **Clock Display**: Set to display the current time on the device (Enable or Disable).
- **Background Image**: Click this checkbox to upload new background images. Click **Add** to locate and add a new image file.

- **Sound**: Click this checkbox to enable and add custom event sounds. Click an event from the list and then click the plus sign (+) to locate and add a new sound file. Click **Add** to add new sound files, **Delete** to remove sound files, or **Play** to preview a selected sound file.

5.1.11.8 T&A tab

The T&A tab allows you to configure the mode and key settings for a BioStation L2 device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



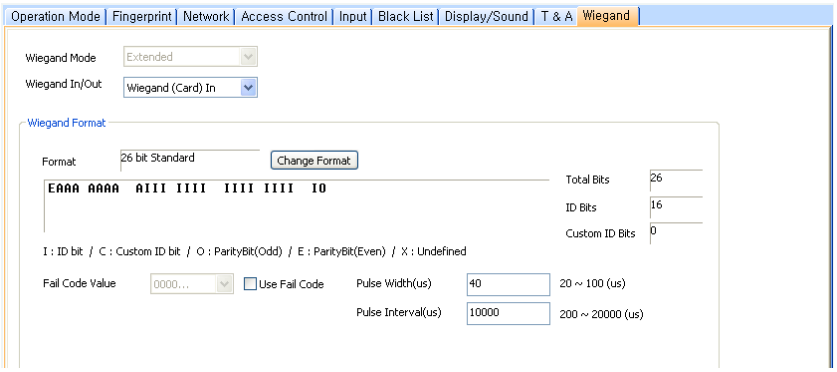
- **T&A Mode**: Set the time and attendance mode:
  - **Not Use**: Disable the time and attendance functions for this device.
  - **Manual:** Users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix**: When a T&A key is pressed, the device will remain in that mode until a different T&A key is pressed.
  - **Auto change**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
  - **Event Fix**: The device will perform only the specified T&A function.
- **T&A Key**: Specify which keys to use for T&A events and the event types associated with them:
  - **Function Key**: Select a function key from the drop-down list to assign a T&A event (*F1-F4*, *EXT01-EXT12)*. If you are using the Event Fix mode, you can click the checkbox to the right to designate a fixed event.
  - **Event Caption**: Enter a caption for the event.
  - **Auto Mode Schedule**: When using the Auto Change mode, you can specify when the event will occur by selecting a timezone in the drop-

down list. For more information on creating a timezone, please see section 3.7.1.

– **Event Type**: Set the type of event to assign to the key (*Not Use*, *Check In*, *Check Out*, *In*, or *Out*). In/Out indicates the general check in/out events during a day whereas Check In/Out indicates the formal check in/out events upon arrival and departure at work—or the first check–in and the last check–out events on that day. When you choose Check In or Check Out, you can enable the "Regard as normal check-in/check-out event" option. If this option is enabled, users who activate the appropriate keys will be regarded as arriving or leaving on time at work even though they actually arrive late or leave early. If you enable the "Only Result" option, they appear being on time on T&A reports but their work time will be calculated correctly based on their actual check in/out time. If you choose *Out*, you can enable the "Add work time after this event" option. If this option is enabled, users activating the appropriate key will be considered working for the remainder of the time slot even if they leave the office early.

5.1.11.9 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioStation L2 device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.13.



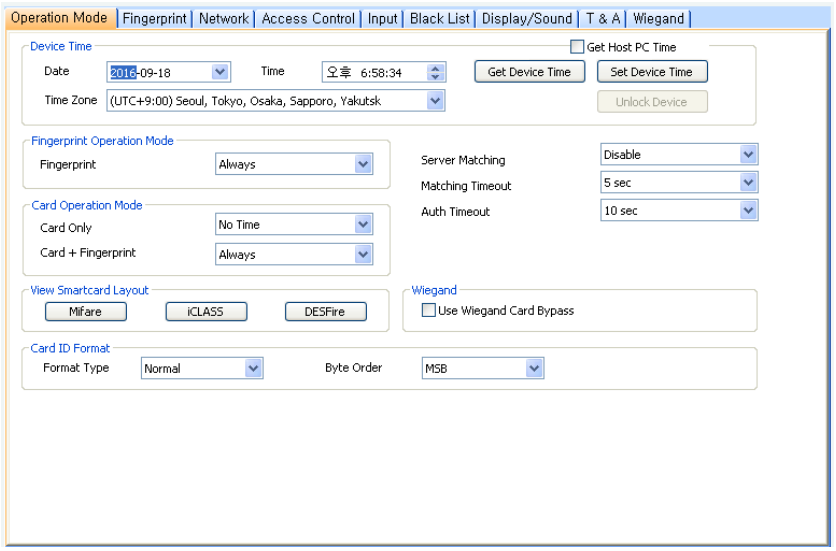
- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Extended*). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the Wiegand input or output:
  – **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.

5.1.12 Customize Settings for BioEntry W2 Devices

The sections below describe the settings available for BioEntry W2 devices. Customize the way BioEntry W2 devices function by changing these settings to suit your particular environment and operational needs.

5.1.12.1 Operation Mode tab

The Operation Mode tab allows you to customize time and various operation modes settings for BioStation L2 devices.



- **Device Time**
  - **Date**: Manually set the device date with a drop-down calendar.
  - **Time**: Manually set the device time.
  - **Time Zone**: Select the time zone you wish to use.
  - **Get Host PC Time**: Check this box to get the time of the local PC which BioStar client program is installed on. The time will be displayed in the **Date** and **Time** spin boxes right below this option and you can set the device's time to match this time by clicking **Set Device Time**.
  - **Get Device Time**: Get the current time displayed by the device.
  - **Set Device Time**: Set the time on the device.
- **Fingerprint Operation Mode**
  - **Fingerprint**: Set the device to require only fingerprint authorization (*Always*, or *No Time*).
- **Card Operation Mode**
  - **Card Only**: Set the device to require only card authorization (*Always*, or *No Time*).

- **Card + Fingerprint**: Set the device to require card plus fingerprint authorization (*Always*, or *No Time*).

- **Other Options**
  - **Server Matching**: Enable this setting to perform user ID, fingerprint or card ID matching at the BioStar server, instead of the device. When this mode is enabled, the devices will send the user ID, fingerprint template or card ID to the server to verify a match. This mode is useful when you have more users than can be downloaded to a device or user information cannot be distributed due to security concerns.
  - **Matching Timeout**: Set the length of time before the device will timeout when trying to identify a fingerprint match within the device itself or via the server (*3, 7, 10, 15, 20, 30 sec*).
  - **Auth Timeout**: Sets the standby time (3 seconds – 20 seconds) for authenticating the next credential when two or more credentials are used.
- **View Smartcard Layout**
  - **MIFARE**: Click this button to view the MIFARE layout used by the device. For more information about configuring MIFARE layouts, please see section 3.6.4.7.
  - **iCLASS**: Click this button to view the iCLASS layout used by the device. For more information about configuring iCLASS layouts, please see section 3.6.4.9.
  - **DESFire**: Click this button to view the DESFire layout used by the device. For more information about configuring DESFire layouts, please see section 3.6.4.8.
- **Card ID Format**
  - **Format Type**: Set the type of pre-processing to occur on card ID data (*Normal* or *Wiegand*). If "Normal" is selected, the card ID data will be processed in its original form. If "Wiegand" is selected, devices will interpret card ID data according to the Wiegand format settings.
  - **Byte Order**: Specify whether to swap ID card data between cards and devices by most significant byte (*MSB*) or least significant byte (*LSB*).

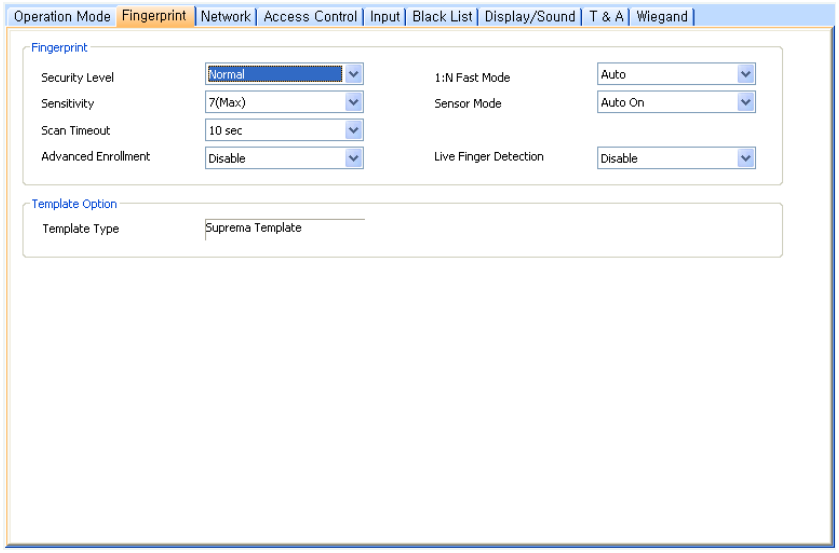
  Note: The device versions 1.x and 2.x have different methods to read card data, but BioStar corrects card data, so card data can be used in the same way. Therefore, MSB/LSB should be set in the same way in the device versions 1.x and 2.x. The card ID displayed by the device may be shown as horizontally reversed, since it is displayed based on Hexa value, but this can be ignored because card data can nevertheless be read correctly.
  - In Double mode, setting option which includes an admin user is supported. In Double mode, door relay will not open unless an admin user authenticates within 15 seconds after a normal user

authenticates. If this option is not activated, the door relay will open when other two users, regardless of whether being a normal user or an admin user.

– **Use Wiegand Card Bypass**: This feature makes the device to send out Card CSN according to Wiegand setting of BioStar without having to conduct a matching. This is designed to be used as a dummy reader in a connection with a third party access control unit through Wiegand. When a card data input is made, the device sends out the data through Wiegand without going through a matching process.

5.1.12.2 Fingerprint tab

The Fingerprint tab allows you to customize fingerprint authorization settings for BioEntry W2 devices.

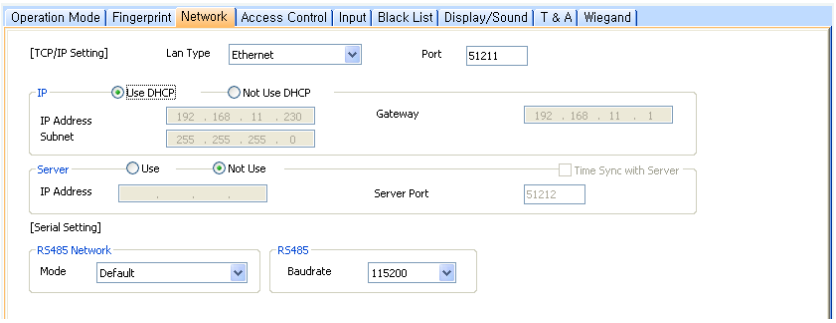


- **Fingerprint**
  - **Security Level**: Set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Sensitivity**: Set the sensitivity of the fingerprint scanner (*0 [Min]* to *7 [Max]*). A higher sensitivity setting will result in more easily captured fingerprint scans, but also increases the sensitivity to external noise.
  - **Scan Timeout**: Set the length of time before the fingerprint scanner will timeout (*1 sec* to *20 sec*). If a user does not place a finger on the device within the timeout period, the authorization will fail.
  - **Advanced Enrollment**: Checks the quality of the scanned fingerprint to avoid the poor quality fingerprint template enrollment. The user will be alerted when the quality of the fingerprint scanned is low and given enrollment instructions.

- **1: N Fast Mode**: Set the device to use Fast Mode to reduce the amount of time required for matching fingerprints (*Auto*, *Normal*, *Fast*, or *Fastest*). Setting Fast Mode to *Auto* will adjust the matching speed according to the number of enrolled templates.
- **Sensor Mode**: If the option is set to **Auto On**, the sensor will automatically go on when it detects a finger. If the option is set to **Always On**, the sensor will always be on.
- **Check Fake Finger**: Set the device to detect the use of fake fingerprints, such as those made from silicon or rubber, and prevent unauthorized access.
- **Template Option**: Displays the global fingerprint template settings. For more information about fingerprint templates, see section 4.9.

5.1.12.3 Network tab

The Network tab allows you to customize network and server settings for BioEntry W2 devices.



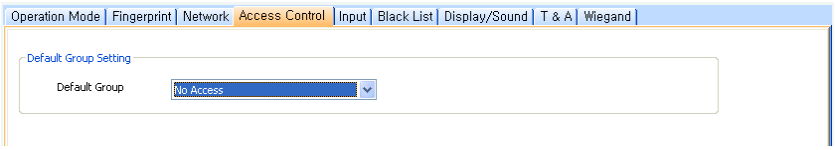
- **TCP/IP Setting**
  - **LAN Type**: Select a type of LAN connection from the drop-down list (*Ethernet*).
  - **Port**: Specify a port to use for the device.
- **IP**
  - **Use DHCP**: Click this option button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP**: Click this option button to disable the dynamic host configuration protocol (DHCP) for this device.
  - **IP Address**: Specify an IP address for the device.
  - **Subnet:** Specify a subnet address for the device.
  - **Gateway**: Specify a network gateway.
- **Server**
  - **Use**: Click this option button to enable the server mode.
  - **Not Use**: Click this option button do disable server settings.
  - **IP Address**: Specify an IP address for the BioStar server.
  - **Server Port:** Specify the port used to connect to the server.

- **Time Sync with Server**: Check this box to synchronize the device' time with the server. The device polls for a time change on the server every one hour and its time will be synchronized with the server when the device's time and the server's time differ by more than 5 seconds.

- **RS485 Network**
  - **Mode**: Set the mode for a device connected via RS485 (*Default*, *Host*, or *Slave*). For more information about RS485 modes, please see sections 3.2.1 and 3.2.2.
  - **Baudrate**: Set the baud rate for a device connected via RS485 (*9600* to *115200*).

5.1.12.4 Access Control tab

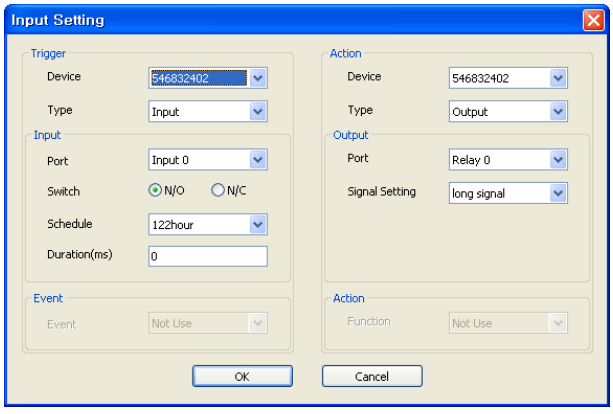
The Access Control tab allows you to customize default access groups for a BioEntry W2 device.



- **Default Group Setting**: Select a default access group to be applied to new users who have not been assigned to another access group.

5.1.12.5 Input tab

The input tab lists input settings you have specified for a BioEntry W2 device. Buttons at the bottom of the tab allow you to add, modify, or delete input settings. To add or modify settings, you must specify them from the **Input Setting** dialog box. For more information about configuring input settings, see section 3.10.3.2.

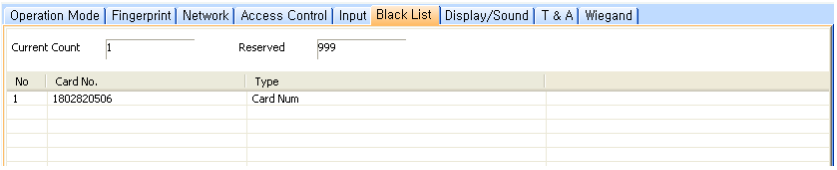


- **Trigger**
  - **Device**: Select a device which a specific event will be monitored.
  - **Type**: Select **Input** or **Event**.
- **Input**: If the **Type** of **Trigger** is set to **Input**, can be set.

  - **Port**: Select an input port (*Input 0*, *Input 1*, or *Tamper*).
  - **Switch**: Click the option buttons to specify the normal position of the input switch (*N/O: normally open* or *N/C: normally closed*).
  - **Schedule**: Set the schedule during which the inputs will be monitored (*Always or No Time*).
  - **Duration(ms)**: Set the duration (in milliseconds) an input signal must last to trigger the specified action.
- **Event**: Set the trigger event. If the **Type** of **Trigger** is set to **Event**, can be set.
- **Action**
  - **Device**: Select a device which performs the action.
  - **Type**: Select **Output** or **Function**.
- **Output**: If the **Type** of **Action** is set to **Output**, can be set.
  - **Port**: Select an output port.
  - **Signal Setting**: Select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Function**: Select an action to associate with the input. If the **Type** of **Action** is set to **Function**, can be set.:
  - **Not Use**: The input port will not be monitored.
  - **Release All Alarms**: Cancel alarms associated with this device.
  - **Restart Device**: Restart the device.
  - **Disable Device**: Disable the device. A disabled device will not communicate with the BioStar server or process fingerprints or card inputs. To enable communication again, an administrator must provide authentication at the device.

5.1.12.6 Black List tab

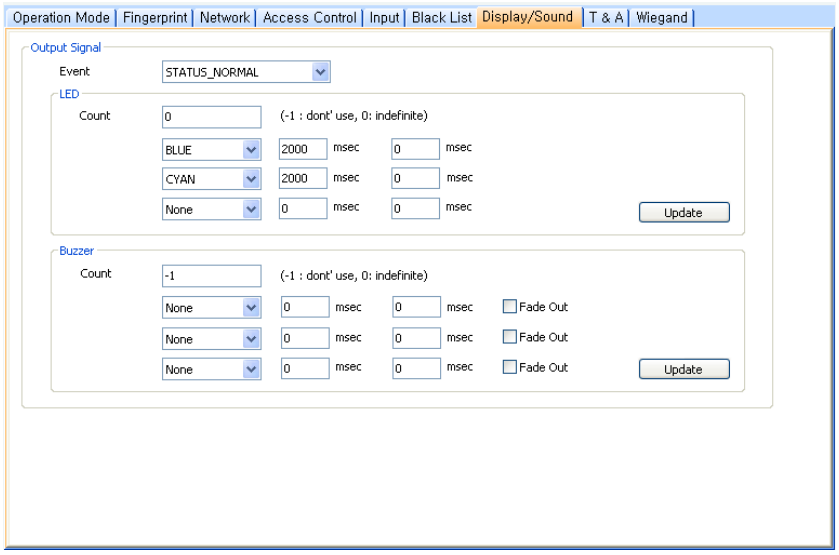
The Black List tab allows you to register user IDs or access card numbers and prevent them from being authenticated with the device.



- **Current Count**: The total number of the user IDs and access cards that have been registered.
- **Reserved** : The remaining number of user IDs and access cards to be registered.

5.1.12.7 Display/Sound tab

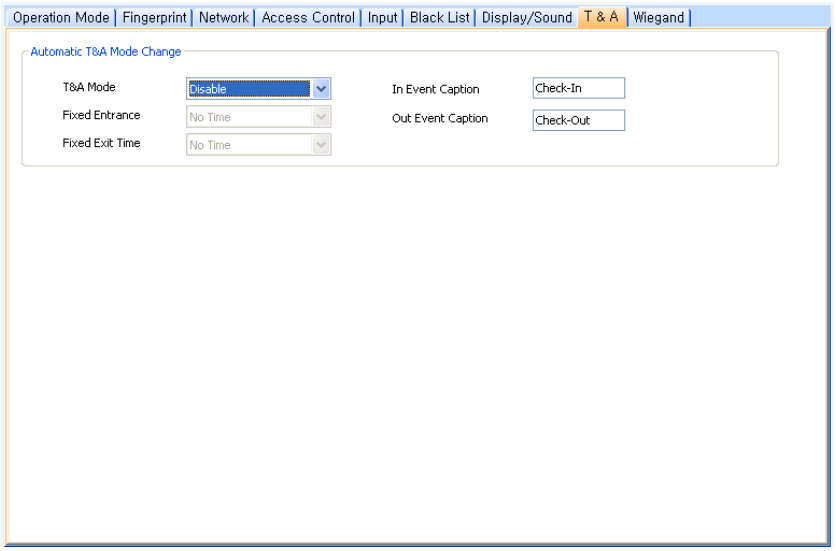
The Display/Sound tab allows you to customize LED and buzzer behaviors by event. To save changes to these settings, you must click **Update** in the corresponding section for each event.



- **Event**: Specify the affected event by selecting it from the drop-down list.
- **LED:** Set the LED behavior for a specified event.
  - **Count**: Enter a number of LED cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the LED.
  - **Colors**: Specify up to three display colors from the drop-down list. The LED will cycle through these colors in order, from top to bottom. Next to each color, enter the duration (in milliseconds) that the LED should display the selected color and the duration (in milliseconds) that the LED should remain off before advancing to the next color in the cycle.
- **Buzzer**: Set the buzzer behavior for a specified event.
  - **Count**: Enter a number of buzzer cycles for the specified event. Enter "0" to enable an infinite loop or "-1" to disable the buzzer.
  - **Volume**: Set up to three tone volumes from the drop-down list (*Low*, *Middle*, or *High*). The buzzer will cycle through these volumes in order, from top to bottom. Next to each volume, enter the duration (in milliseconds) that the buzzer should maintain the selected volume and the duration (in milliseconds) that the buzzer should remain off before advancing to the next volume in the cycle.
- **Fade Out**: Set the tone volume to fade out before advancing to the next volume in the cycle by clicking this checkbox.

5.1.12.8 T&A tab

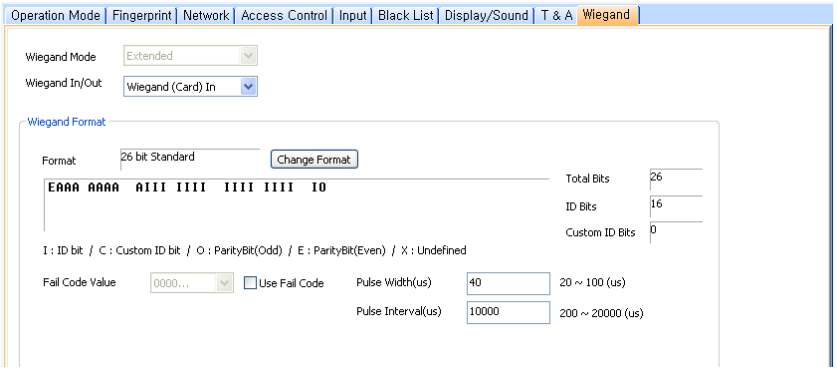
The T&A tab allows you to configure the mode settings for a BioEntry W2 device. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also apply the same settings to other devices by clicking **Apply to Others**.



- **T&A Mode**: Set the time and attendance mode:
  - **Disable**: Disable the time and attendance functions for this device.
  - **Fixed In:** The device will perform only the check in event.
  - **Fixed Out**: The device will perform only the check out event.
  - **Auto**: The device will automatically change T&A modes to correspond with the functions specified for a time period.
- **Fixed Entrance**: When using the **Auto** for **T&A Mode**, you can specify when the check in event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
- **Fixed Exit Time**: When using the **Auto** for **T&A Mode**, you can specify when the check out event will occur by selecting a timezone in the drop-down list. For more information on creating a timezone, please see section 3.7.1.
- **In Event Caption**: Enter a caption for the check in event.
- **Out Event Caption**: Enter a caption for the check out event.

5.1.12.9 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioEntry W2 device. Click **Change Format** to launch the Wiegand Configuration wizard. For more information on configuring the Wiegand format, see section 3.2.16.



- **Wiegand Mode**: Set the mode of Wiegand input to use when reading card ID data (*Extended*). The Extended mode will allow RF card readers to operate independently, which allows them to be associated with doors, included in zones, and leave logs with their own device IDs.
- **Wiegand In/Out**: Assign the Wiegand input or output:
  - **Wiegand (Card) In**: The ID field of the Wiegand string is interpreted as a card ID.

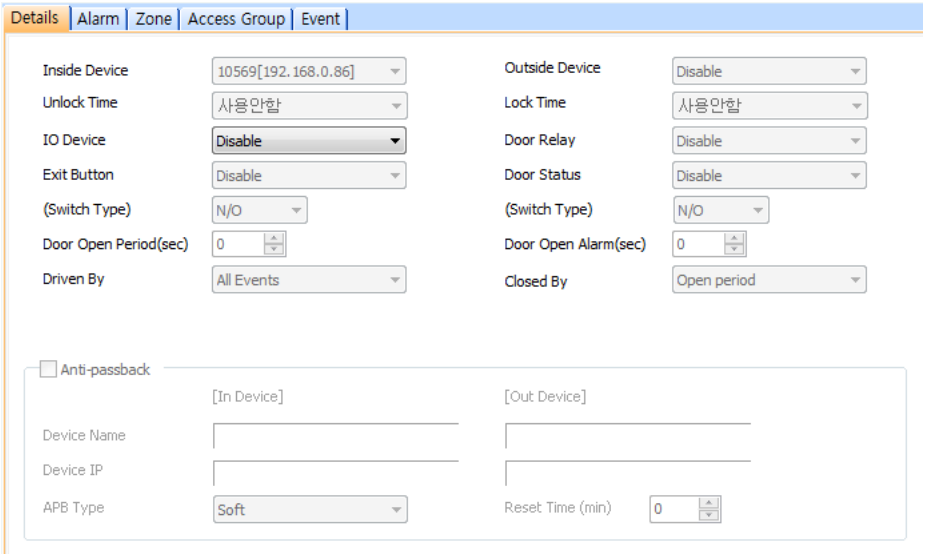
5.2 Customize Door Settings

The sections below describe the settings available for doors that have been added to the BioStar system. Customize the way these doors function by changing settings to suit your particular environment and operational needs. To access the tabs described below, click **Doors** in the shortcut pane, then click a door name.

Attention: A 2.x device (BioStation A2, BioStation 2, BioStation L2, BioEntry W2) cannot configure the door together with a 1.x device (BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation).

5.2.1 Details tab

The Details tab allows you to specify which devices are used on the inside or outside of a door, how the devices control the door, and anti-passback features. When connecting two devices to a single door, the devices should be connected to each other by RS485. In this case, the I/O ports of only one device can be used. Specify which device's I/O ports to use in the “IO Device” drop-down list.



- **Inside Device**: Select a device to use on the inside of the door.
- **Outside Device**: Select a device to use on the outside of the door.
- **Unlock Time**: Select a schedule when the door should normally be unlocked. During this time, door relays are active.
- **Lock Time**: Select a schedule when the door should normally be locked. During this time, door relays are inactive.
- **IO Device**: When using two devices on a single door, specify which device's IO ports will be used.
- **Door Relay**: Select a door relay.
- **Exit Button**: Select a device input to use for an exit button (*Disable* or *Input 0* and *Input 1* for each device added).
- **(Switch Type)**: Set the normal position of the input used for an exit button (*N/O-normally open* or *N/C-normally closed*).
- **Door Status**: set an input for a sensor that detects the current status of the door.
- **(Switch Type)**: Set the normal position of the input used for a door status sensor (*N/O-normally open* or *N/C-normally closed*).
- **Door Open Period (sec)**: Set the duration (in seconds) that a door relay should be activated when a door is opened. After this duration, the relay will stop sending the signal to open the door. The default is three seconds.
- **Door Open Alarm (sec)**: Set the duration (in seconds) that a door can remain open before an alarm will sound.
- **Driven by**: Select types of events that will trigger associated devices to open the door.
  - **All Events (default)**: Associated devices will open the door on any successful authorization events.
  - **TNA + AUTH**: Associated devices will open the door on successful T&A or credential authorization events or T&A authorization events. To use this option, you must select the Use Relay checkbox in the T&A tab. This option is only available for BioStation, BioLite Net, X-Station, BioStation T2, FaceStation, and

BioStation 2, BioStation A2, and BioStation L2 devices. For more information about configuring T&A settings, see section 5.1.1.9, 5.1.3.9, 5.1.6.10, 5.1.7.11, 5.1.8.10, 5.1.9.9, 5.1.10.9, and 5.1.11.8.

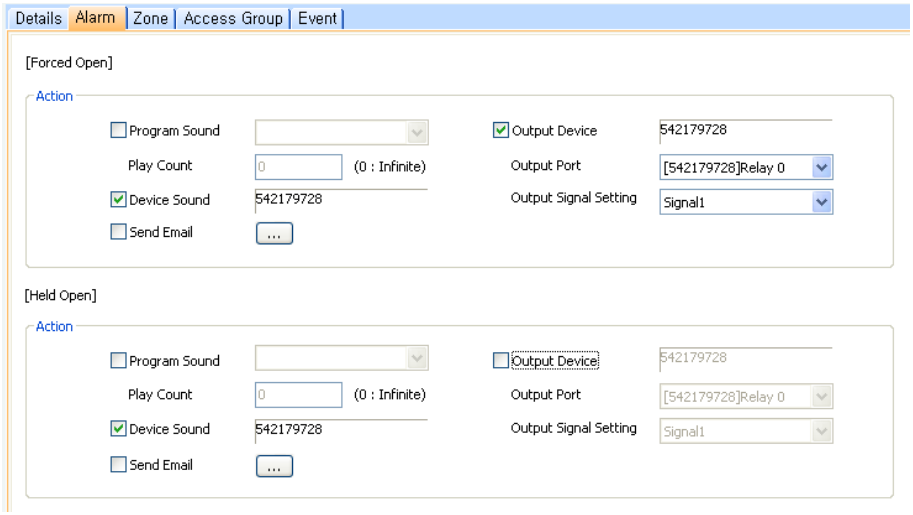
- **AUTH**: Associated devices will open the door only on successful credential authorization events.
- **TNA**: Associated devices will open the door only on successful T&A authorization events. To use this option, you must select the Use Relay checkbox in the T&A tab. This option is only available for BioStation, BioLite Net, X-Station, BioStation T2, FaceStation, BioStation 2, BioStation A2, and BioStation L2 devices. For more information about configuring T&A settings, see section 5.1.1.9, 5.1.3.9, 5.1.6.10, 5.1.7.11, 5.1.8.10, 5.1.9.9, 5.1.10.9, and 5.1.11.8.
- **Disabled**: Associated devices will not open the door, regardless of the attempted authorization events.

- **Closed by**: Select an option for closing the door.
  - **Open Period**: The BioStar system will close the door after the period specified in the *Door Open Period (sec)* field.
  - **Open Period+Status**: The BioStar system will attempt to close the door based on door status (if you have connected door sensors and the system can detect that the door is open). If door sensors are not connected or the system is unable to detect the door status, the system will close the door after the period specified in the *Door Open Period (sec)* field. This setting is useful when used with revolving doors, for example, to prevent someone from following an authorized person through the door.
- **Anti-passback**: Click the checkbox to activate the anti-passback feature (only available when using both an inside and an outside device).
  - **Device Name**: This field is populated automatically.
  - **Device IP**: This field is populated automatically.
  - **APB Type**: Set the type of anti-passback restriction to use (Soft or Hard).
  - **Reset Time (min)**: Set the duration (in minutes) that must pass before the anti-passback status is reset. The default reset time is 0—at this setting, the anti-passback status will not be reset.
- **Unlock Trigger Option**
  - Unlock Trigger Option: Unlock Trigger is supported in the 'Details' tab in the door setting. This feature allows the door to be remained open during Unlock Time only after an Admin User or Normal User identification.
    Note: Supported Firmware Versions: BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3. 2.x devices (BioStation 2, BioStation A2, BioStation L2, BioEntry W2) are not supported.
    Note: Unlock Trigger is not supported when two devices (Host/Slave device or 3rd Party Wiegand reader) are configured for one door and Unlock Trigger was made from the slave device. And when the case that 3rd Party Wiegand reader is configured for one door is not supported. And it's supported only when a triger was made from one Host device.
- **Minimum Input Duration**

– Minimum Input Duration: This feature can be activated from 'Details' tab in the door setting. When this option is in use, the device accepts input signal only when the signal continues more than a certain period of time designated by the FW fix. This option is activated with the latest FW and shown Use or Not Use.
Note: Supported Firmware Versions: BioStation 1.93, BioStation T2 1.3, FaceStation 1.3, BioEntry Plus 1.6, BioEntry W 1.2, BioLite Net 1.4, Xpass 1.3.

5.2.2 Alarm tab

The Alarm tab allows you to specify alarm actions for doors that are forced open or held open. A forced open alarm occurs when a door is forcibly opened without any authentication at the device. A held open alarm occurs when a door remains open longer than the duration specified in the system settings.



- **Action**
  - **Program Sound**: Activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound**: Activate and select a sound to be emitted by devices connected to the door.
  - **Send Email:** Activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device**: Activate and select a device to output an alarm signal.
  - **Output Port**: Select an output port to use when sending the alarm signal.
  - **Output Signal Setting**: Select an output signal to send.

5.3 Customize Zone Settings

Customize the way zones function by changing the settings to suit your particular environment and operational needs. To access the tabs described below, click **Doors** in the shortcut pane, then click a zone name.

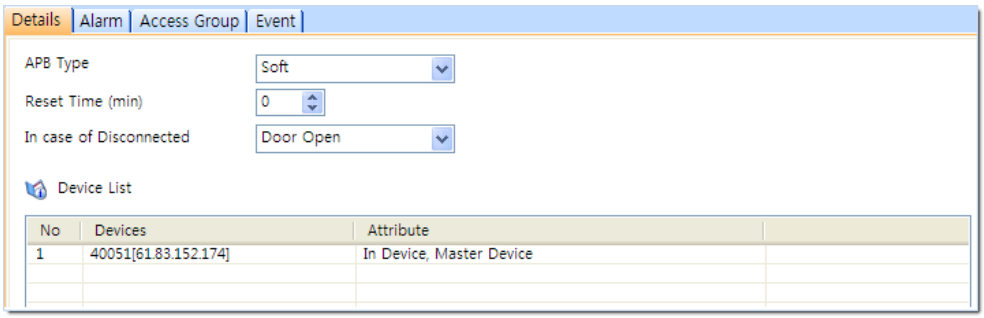
5.3.1 Customize Settings for Anti-Passback Zones

The sections below describe the settings available for anti-passback zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

Attention: A 2.x device (BioStation A2, BioStation 2, BioStation L2, BioEntry W2) cannot configure a zone together with a 1.x device (BioStation, BioEntry Plus, BioEntry W, BioLite Net, Xpass, Xpass S2, X-Station, BioStation T2, FaceStation). Also, BioStation A2, BioStation 2, BioStation L2 and BioEntry W2 can configure only a dual access device zone and a fire alarm zone.

5.3.1.1 Details tab

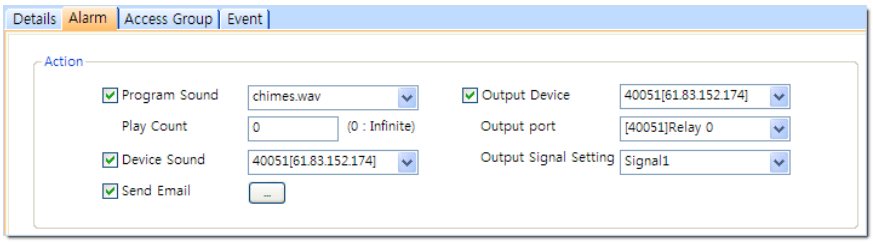
The Details tab allows you to specify which anti-passback type to use for a zone and the reset period for the anti-passback feature.



- **APB Type**: Select a type of anti-passback restriction to apply (*Soft* or *Hard*).
- **Reset Time (min)**: Set the duration (in minutes) that must pass before the anti-passback status is reset. The default reset time is 0—at this setting, the anti-passback status will not be reset.
- **In case of Disconnected**: Set how doors in the zone should behave if communication is lost between the master and member devices.

5.3.1.2 Alarm tab

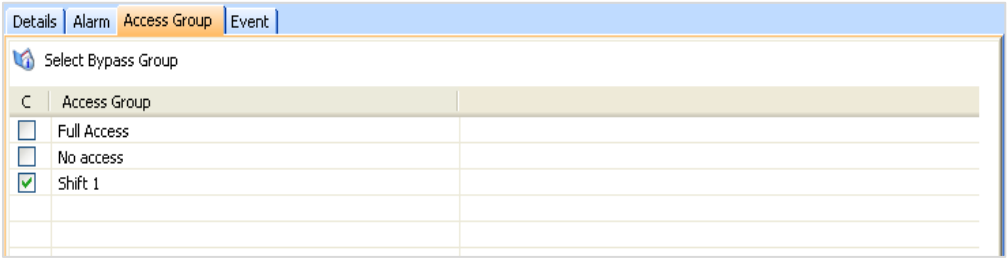
The Alarm tab allows you to specify alarm actions and an output device for an anti-passback zone.



- **Action**
  - **Program Sound**: Activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound**: Activate and select a sound to be emitted by devices connected to the door.
  - **Send Email**: Activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device**: activate and select a device to output an alarm signal.
  - **Output Port**: Select an output port to use when sending the alarm signal.
  - **Output Signal**: Select an output signal to send.

5.3.1.3 Access Group tab

The Access Group tab allows you to specify access groups that can bypass normal restrictions for the zone. To grant bypass rights to an access group, select a group and click **Apply** at the bottom right of the Zone pane.

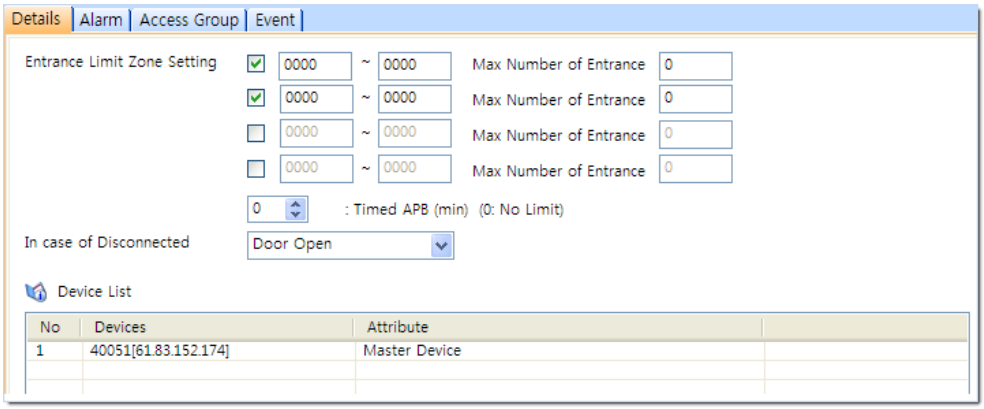


5.3.2 Customize Settings for Entrance Limit Zones

The sections below describe the settings available for entrance limit zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.2.1 Details tab

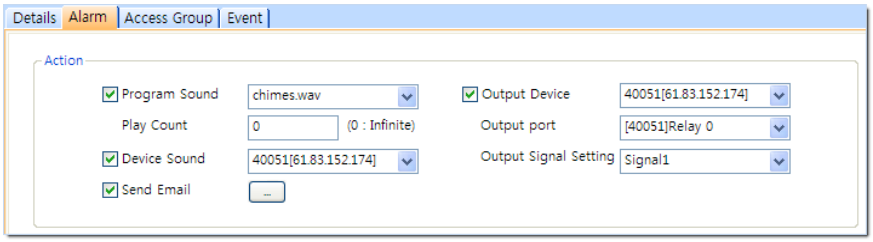
The Details tab allows you to specify entrance limits and a schedule for the zone restrictions.



- **Entrance Limit Zone Setting**: Click the checkbox to enable an entrance limit setting, and then specify the effective hours for the entrance limit.
- **Max Number of Entrance**: Set the maximum number of entries allowed during the specified time limit.
- **Timed APB (min)**: Specify a time limit for re-entry into a zone.
- **In case of Disconnected**: Set how doors in the zone should behave if communication is lost between the master and member devices.

5.3.2.2 Alarm tab

The Alarm tab allows you to specify alarm actions and an output device for an entrance limit zone.

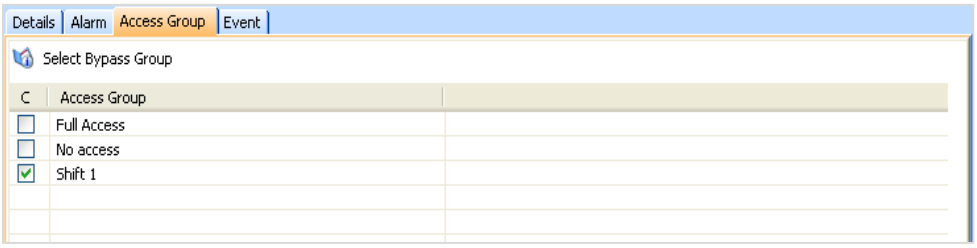


- **Action**
  - **Program Sound**: Activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound**: Activate and select a sound to be emitted by devices connected to the door.
  - **Send Email**: Activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.

- **Output Device**: Activate and select a device to output an alarm signal.
- **Output Port**: Select an output port to use when sending the alarm signal.
- **Output Signal**: Select an output signal to send.

5.3.2.3 Access Group tab

The Access Group tab allows you to specify access groups that can bypass normal restrictions for the zone. To grant bypass rights to an access group, select a group and click **Apply** at the bottom right of the Zone pane.



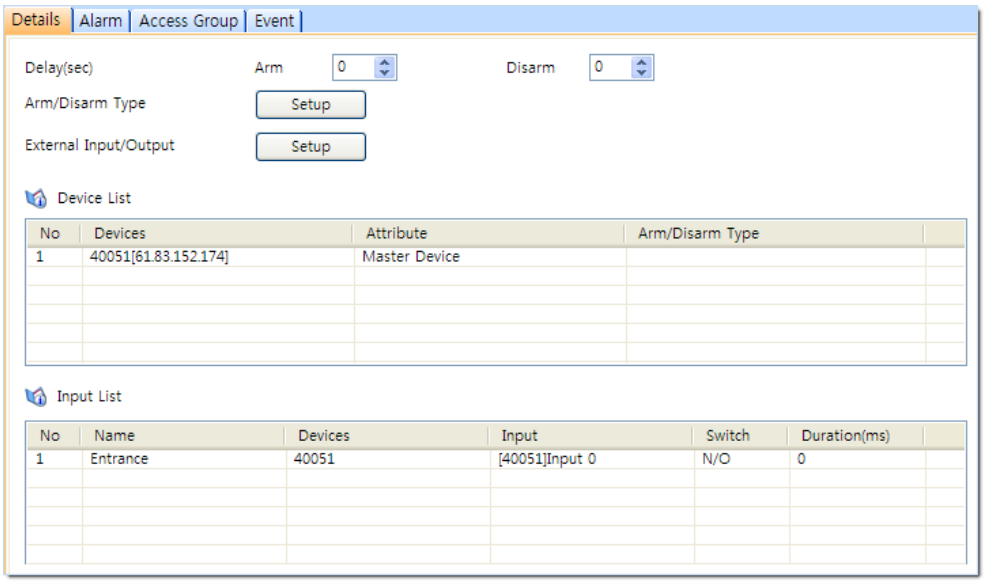
5.3.3 Customize Settings for Alarm Zones

The sections below describe the settings available for alarm zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

Attention: Arm/disarm cannot be set for a door or a zone configured with BioStation A2, BioStation 2, BioStation L2 and BioEntry W2.

5.3.3.1 Details tab

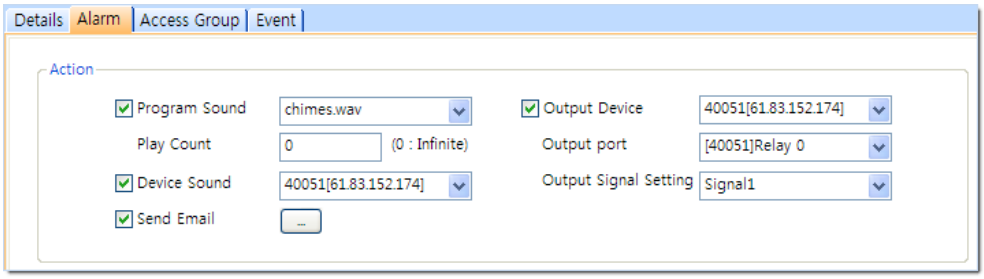
The Details tab allows you to specify alarm delays and arm/disarm types for alarm zones.



- **Delay (sec)**
  - **Arm**: Set the length of time (in seconds) to delay before arming the zone.
  - **Disarm**: Set the length of time (in seconds) to delay before disarming the zone.
- **Arm/Disarm Type**: Specify settings for arming or disarming zones. For more information for configuring arm and disarm settings, see 3.5.2.5. For more information on setting up alarms, see section 3.10.
- **External Input/Out**: Specify settings for enabling the BioStar system to antomatically arming or disarming zones. For more information on configuring external input/output settings, see 3.5.2.6. For more information on setting up alarms, see section 3.10.

5.3.3.2 Alarm tab

The Alarm tab allows you to specify alarm actions and an output device for an alarm zone.



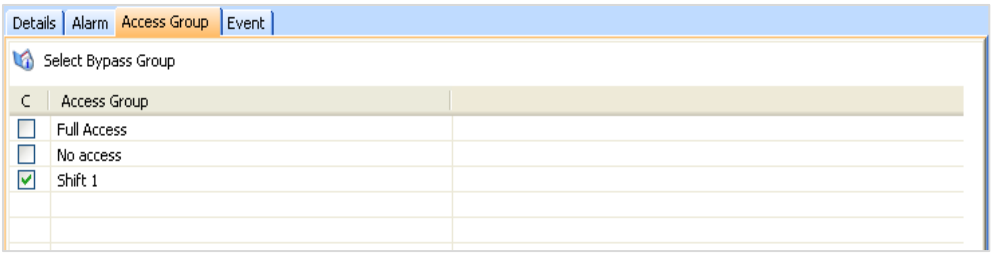
- **Action**
  - **Program Sound**: Activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0,

the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.

- **Device Sound**: Activate and select a sound to be emitted by devices connected to the door.
- **Send Email**: Activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
- **Output Device**: Activate and select a device to output an alarm signal.
- **Output Port**: Select an output port to use when sending the alarm signal.
- **Output Signal**: Select an output signal to send.

5.3.3.3 Access Group tab

The Access Group tab allows you to specify access groups that can arm and disarm zones. To grant disarm authorization to an access group, select a group and click **Apply** at the bottom right of the Zone pane.

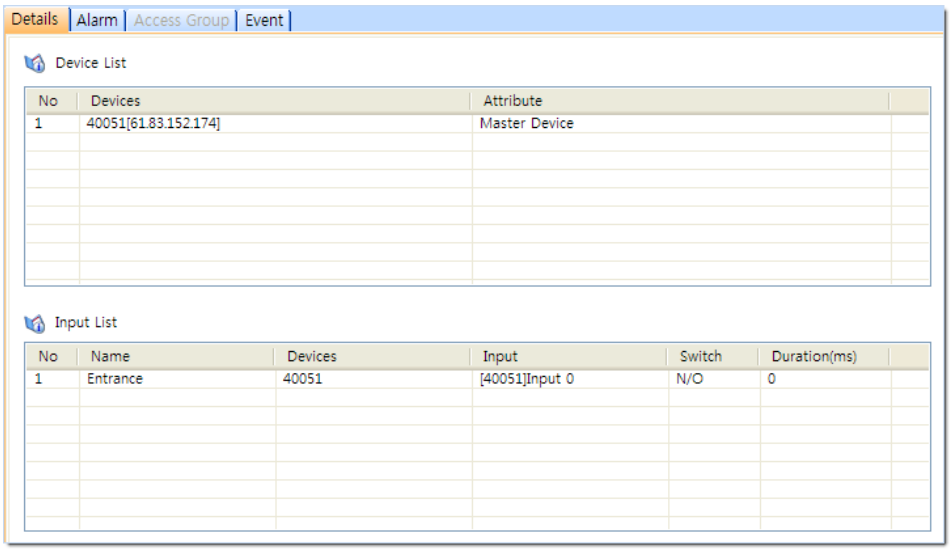


5.3.4 Customize Settings for Fire Alarm Zones

The sections below describe the settings available for fire alarm zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

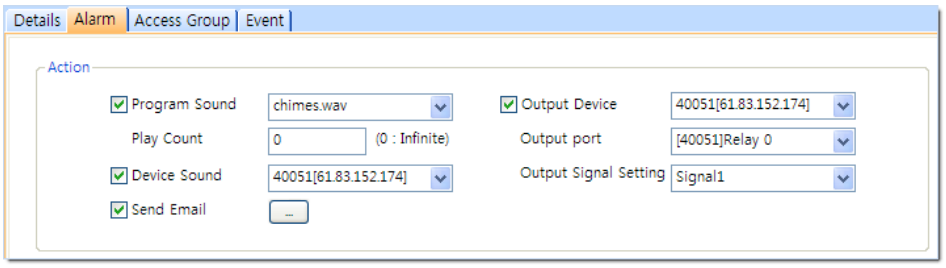
5.3.4.1 Details tab

The Details tab allows you to add or delete devices in the Device List and inputs to the Input List. To add or delete devices, see section 3.5.2.2.



5.3.4.2 Alarm tab

The Alarm tab allows you to specify alarm actions and an output device for a fire alarm zone.



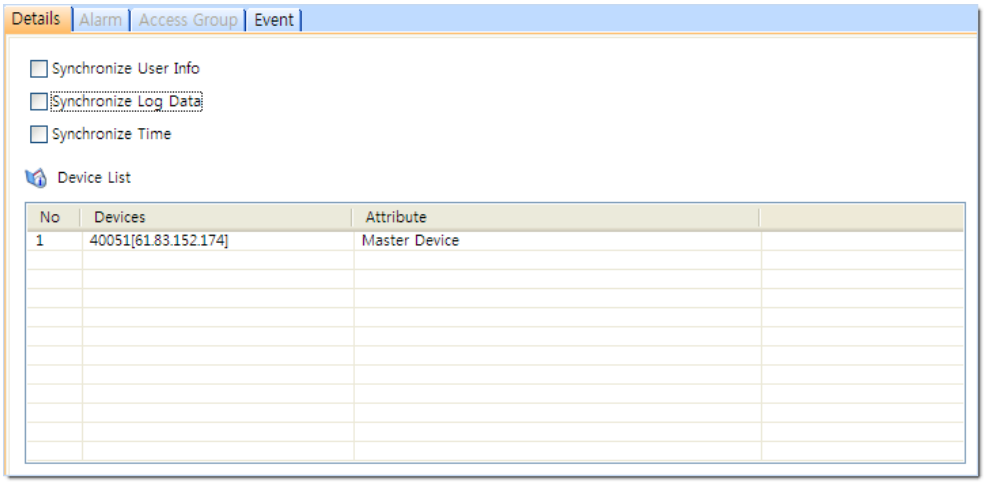
- **Action**
  - **Program Sound**: Activate and select a sound from the drop-down list to be emitted by the BioStar program. Then, specify the duration ("play count") of the sound in seconds. If you set the Play Count to 0, the specified sound will play until someone with administrative privileges manually stops the sound via the Realtime Monitoring tab in the Monitoring pane. To add custom sounds to the list, see section 3.10.1.2.
  - **Device Sound**: Activate and select a sound to be emitted by devices connected to the door.
  - **Send Email**: Activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.10.2.
  - **Output Device**: Activate and select a device to output an alarm signal.
  - **Output Port**: Select an output port to use when sending the alarm signal.
  - **Output Signal**: Select an output signal to send.

5.3.5 Customize Settings for Access Zones

The sections below describe the settings available for access zones. These zones are used to synchronize user data, so the Alarm and Access Group tabs are unavailable. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.5.1 Details tab

The Details tab allows you to add devices to the Device List.



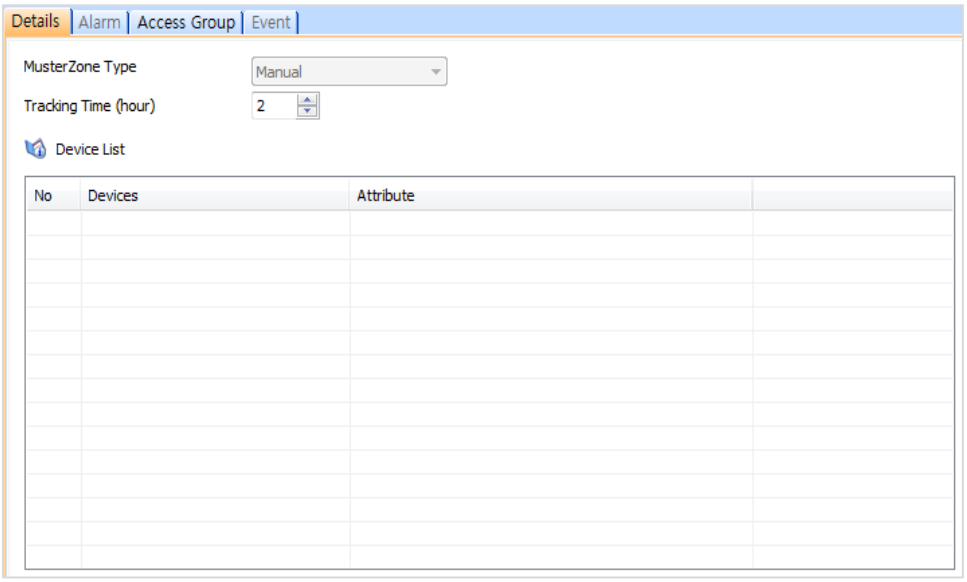
- **Synchronize User Info**: Click this checkbox to automatically propagate user information to other devices.
- **Synchronize Log Data**: Click this checkbox to automatically write all log records to the master device (for member devices in the zone).
- **Synchronize Time**: Click this checkbox to synchronize the time of devices in the zone.

5.3.6 Customize Settings for Muster Zones

The sections below describe the settings available for muster zones. These zones are used to monitors user locations, so the Alarm tab is unavailable. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

5.3.6.1 Details tab

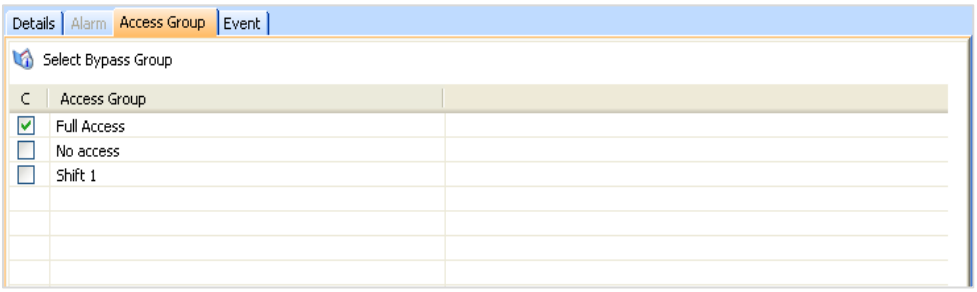
The Details tab allows you to add devices to the Device List.



- **Muster Zone Type**: By default, set to *Manual*. You can check for the people who were present in a specified area for a specific time period. Please see 4.1.1 to see how to manually check attedance of people.
- **Tracking Time (hour)**: Specify how far (in hours) people are monitored for their in/out activities in the zone. For example, if you set this value to 8, you can track a record of attendace since 8 hours ago.

5.3.6.2 Access Group tab

The Access Group tab allows you to specify access groups that belong to a muster zone. To assign access groups to a muster zone, select a group and click **Apply** at the bottom right of the Zone pane.



5.3.7 Customize Settings for Interlock Zones

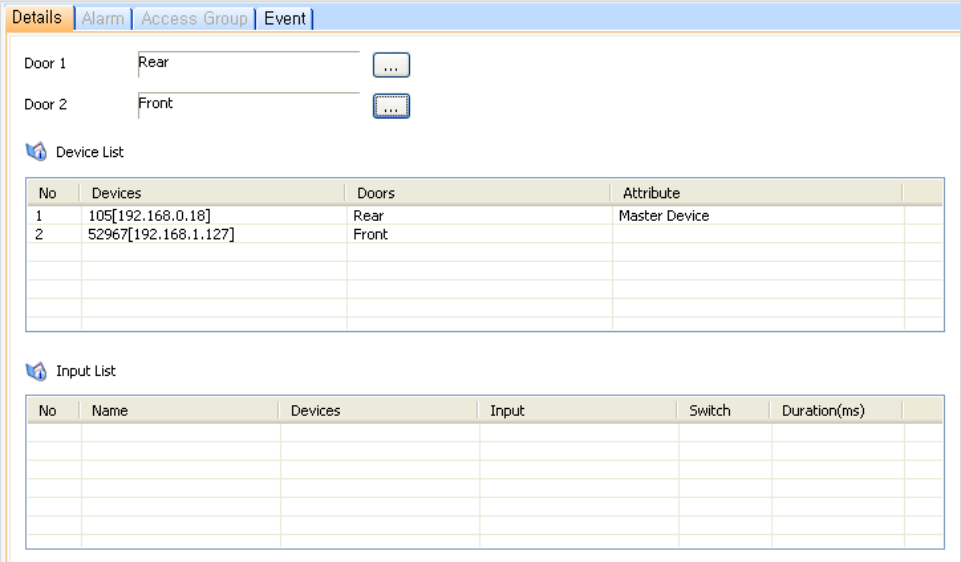
The sections below describe the settings available for interlock zones. Customize the way the zone functions by changing these settings to suit your particular environment and operational needs.

Interlock zones works only with the following device firmware versions:

- FaceStation V1.3 or later, BioStation T2 V1.3 or later, BioStation V1.9 or later, BioEntry Plus V1.5 or later, BioEntry W V1.0 or later, BioLite Net V1.3 or later, Xpass V1.2 or later, and X-Station V1.3 or later.
- Interlock zones are not supported for D-Station, BioStation 2, BioStation A2, BioStation L2 and BioEntry W2.

5.3.7.1 Details tab

The Details tab allows you to specify which doors to use for either side of the interlock zone. Once added, the door names and device IDs will appear in the Device List.



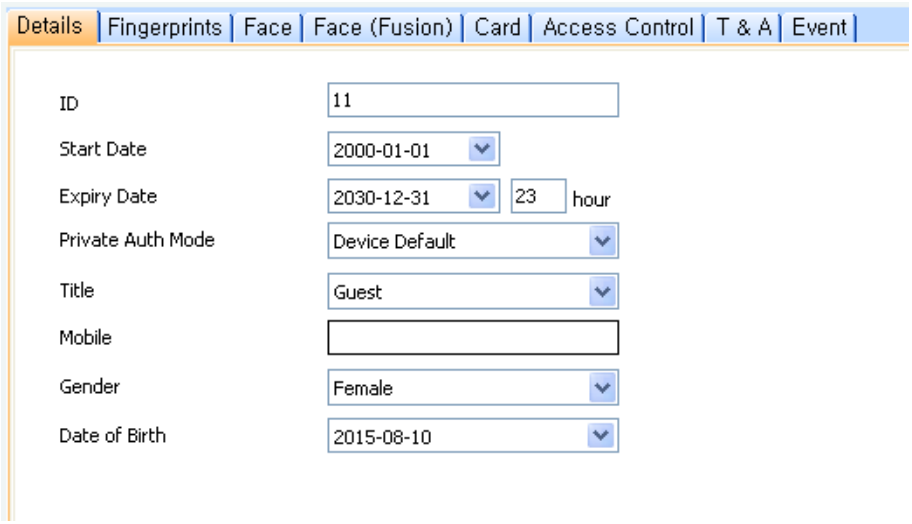
- **Door 1**: Click the ellipsis (…) button to select door 1 of the interlock area. Doors without associated devices cannot be added to the interlock zone.
- **Door 2**: Click the ellipsis (…) button to select the device on door 2 of the interlock area. Doors without associated devices cannot be added to the interlock zone.

5.4 Customize User Settings

Customize various settings for users, including personal details, fingerprint information, and access card information. To access the tabs described below, click **Users** in the shortcut pane, then click a user name.

5.4.1 Details Tab

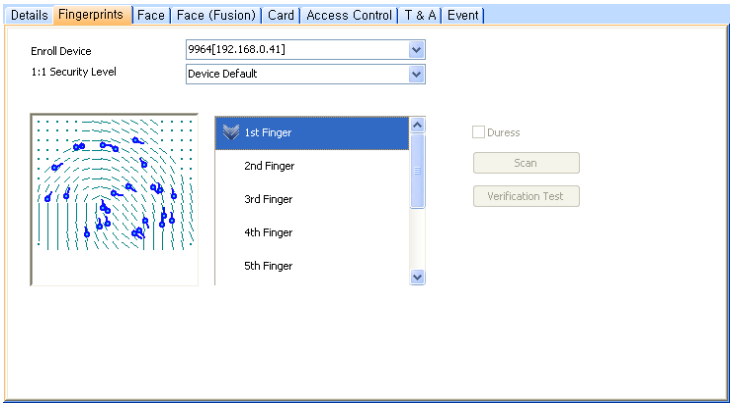
The Details tab allows you to specify personal information about a user and the valid dates of a user account. To edit these fields, see section 4.5.3.



- **ID**: Enter an identification number for a user.
- **Start Date**: Set a beginning date that the user can obtain authorization via the BioStar system.
- **Expiry Date**: Set a date that the user's account will expire (you can also specify the hour that the account will expire).
- **Private Auth Mode**: Set the authorization method for the user (*Device Default*, *Fingerprint*, *Fingerprint + Password*, *Card Only*, *Card + Fingerprint*, *Card + Password*, *Card + Fingerprint/Password*, *Card + Fingerprint + Password*, *ID + Fingerprint*, *ID + Password*, *ID + Fingerprint/Password*, *ID + Fingerprint + Password*). If you set the method to "Device Default," the authentication mode will be determined by operation mode settings of the device.
- **Title**: Select a title for the user (*Guest*, *President*, *Director*, *General Manager*, *Chief*, *Assistant Manager*, or custom title).
- **Mobile**: Enter a mobile telephone number for a user.
- **Gender**: Select a user's gender.
- **Date of Birth**: Select a user's date of birth from the drop-down calendar.

5.4.2 Fingerprints Tab

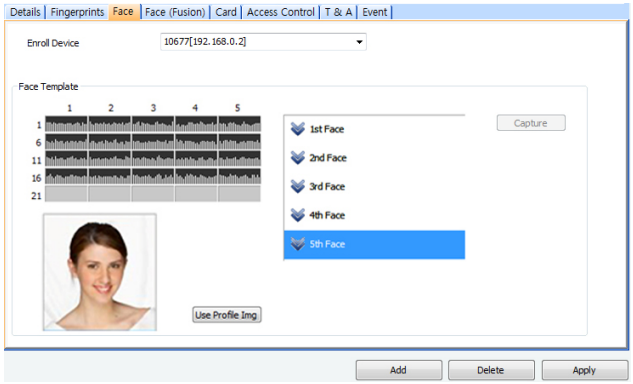
The Fingerprints tab allows you to specify which type of scanner to use for enrollment and the security level to apply. This tab can also be used to test for fingerprint matches and register duress fingerprints. For more information about registering fingerprints, see section 3.6.2.



- **Enroll Device**: Select a device to use for scanning fingerprints.
- **1: 1 Security Level**: Select a security level to use for fingerprint authorization (*Device Default* and *Lowest [1/1,000]* to *Highest [1/10,000,000]*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
- **Duress**: set a fingerprint template to be used as a duress finger (the duress finger will activate alarms when used to gain entry).

5.4.3 Face Tab

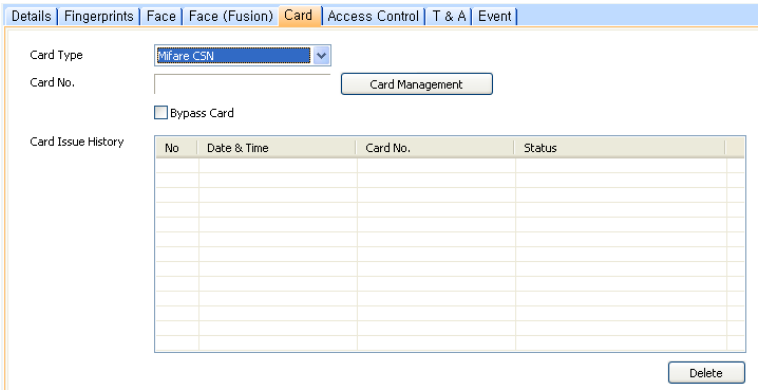
The Face tab allows you to specify a FaceStation device to use for storing face templates of users. When you sucessfully capture faces(up to 5 per user), the FaceStation device transfers 25 face templates to the BioStar. During authentication, any face template that receives a higher score than one of the registered face templates will replace the old one. For more information about capturing face images, see section 3.6.3.



- **Enroll Device**: Select a device to use for capturing face images.

5.4.4 Card Tab

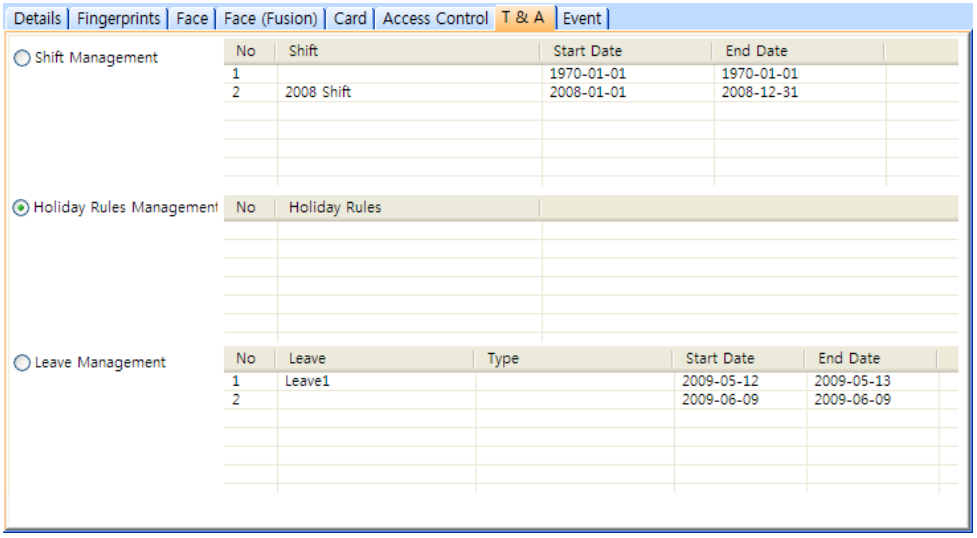
The Card tab allows you to specify card types and IDs and issue cards to users. For more information about issuing cards, see section 3.6.4.



- **Card Type**: Select a type of access card to issue (*Mifare CSN, Mifare Template, EM 4100, HID Prox, iCLASS CSN, or iCLASS Template*).
- **Card ID**: Displays the card ID number when a card is issued.
- **Custom ID**: Enter a custom ID for the card.

5.4.5 T&A Tab

The T&A tab allows you to specify which shifts, holiday rules, and leave periods apply to a user. To add new details, click **Add** at the bottom of the tab. To save changes to time and attendance settings, you must click **Apply** at the bottom of the tab. You can also remove entries by highlighting the entry and clicking **Delete**. For more information about configuring time and attendance, please see section 3.9.



- **Shift Management**: Specify which shifts apply to the user.
- **Holiday Rules Management**: Specify which holiday rules apply to the user.
- **Leave Management**: Specify leave for the user.

06 Technical Support

If you have any questions regarding this document or BioStar software, please contact technical support at **support@supremainc.com**.

Please provide the following information for prompt and easy assistance:

- Contact information and available times
- Version of BioStar and device model name (e.g. BioStar 1.93, BioStation 2)
- Error messages and description on problems

07 Open Licenses

AES

FIPS-197 compliant AES implementation Copyright (C) 2006-2007 Christophe Devine

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License, version 2.1 as published by the Free Software Foundation.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

The AES block cipher was designed by Vincent Rijmen and Joan Daemen.

http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

MD5

MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm
Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

OpenSSL

LICENSE ISSUES
==========
The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

7. Open Licenses

==========
Copyright (c) 1998-2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==========

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).
This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.
This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

7. Open Licenses

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

SHA-256

FIPS-180-2 compliant SHA-256 implementation
Copyright (C) 2006-2007 Christophe Devine

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License, version 2.1 as published by the Free Software Foundation.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

The SHA-256 Secure Hash Standard was published by NIST in 2002.
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

Libiconv

Copyright (C) 1999-2003 Free Software Foundation, Inc.
This file is part of the GNU LIBICONV Library.

The GNU LIBICONV Library is free software; you can redistribute it and/or modify it under the terms of the GNU Library General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

The GNU LIBICONV Library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Library General Public License for more details.

You should have received a copy of the GNU Library General Public License along with the GNU LIBICONV Library; see the file COPYING.LIB.
If not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

Libxml2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PTHREADS-WIN32

==========
Pthreads-win32 is free software, distributed under the GNU Lesser General Public License (LGPL). See the file 'COPYING.LIB' for terms and conditions. Also see the file 'COPYING' for information specific to pthreads-win32, copyrights and the LGPL.

What is it?

7. Open Licenses

Pthreads-win32 is an Open Source Software implementation of the Threads component of the POSIX 1003.1c 1995 Standard (or later) for Microsoft's Win32 environment. Some functions from POSIX 1003.1b are also supported including semaphores. Other related functions include the set of read-write lock functions. The library also supports some of the functionality of the Open Group's Single Unix specification, version 2, namely mutex types, plus some common and pthreads-win32 specific non-portable routines (see README.NONPORTABLE).

Zlib
zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.5, April 19th, 2010

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly Mark Adler
jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

Glossary

access card: A card that can be used to grant or restrict access to a specific area. BioStar supports MIFARE®, EM4100, HID proximity, iCLASS®, and FeliCa® cards. See also: proximity card.

access control system: A system of physical mechanisms and controls that permit or deny access to a particular resource or physical area. BioStar is an IP-based biometric access control system.

alarm zone: A grouping of devices that is used to protect a physical area. BioStar monitors input points in an alarm zone and triggers alarms when intrusion or tampering is detected.

anti-passback: A security protocol that prevents a user from providing unauthorized entrance to another user via an access card or fingerprint. See also: timed anti-passback.

biometrics: Biometrics refers to the use of physical characteristics for verification or authorization. BioStar incorporates Suprema's award-winning fingerprint recognition technology to provide biometric authentication of a user's identity and authorization to gain access to restricted areas.

bypass group: A group of users that can bypass normal restrictions for a zone.

client: BioStar client software allows an operator to connect remotely to the BioStar server and control connected devices. An operator ID and password are required to access the system via a client.

department: A division of an organization used to group employees. The use of departments is not necessary, but may be helpful to organize large numbers of employees.

device: In this guide, the word "device" refers to any Suprema product supported by the BioStar system. Supported devices include BioStation, BioStation Mifare, BioStation HID, DStation, BioEntry Plus/BioEntry W, BioEntry Plus Mifare/BioEntry W Mifare, BioEntry Plus iCLASS, BioEntry Plus HID, BioLite Net, Xpass, and BioMini USB terminals, as well as the Secure I/O device.

distributed intelligence: In the BioStar system, the authorization database is distributed to each terminal, so that authorization is faster and can continue even when other parts of the system are offline.

Glossary

door: Doors are the physical barriers that provide entry into a building or space. At least one device must be connected to a door to provide access control, but two devices can be connected to support anti-passback and other features, such as door relays, alarm relays, exit switches, and sensors.

duress finger: This term refers to an enrolled fingerprint that will activate silent alerts when a candidate is under duress. In the typical duress scenario, a perpetrator forces the candidate to gain access by force or threat of harm. The candidate gains access by means of his or her "duress finger," which allows access and simultaneously triggers the alarm or alert actions you specify.

enrollment: The process of creating a user account and capturing images of fingerprints or issuing access cards.

entrance limit: The maximum number of times a user can gain authorization to a specific area. The entrance limit can be related to a time period so that users are limited to certain number of entries during office hours, for example.

ESSID: Extended Service Set ID. The ESSID is the name of a wireless network access point. It allows one wireless network to be clearly distinguishable from another. ESSID is one type of SSID (the other being BSSID).

face recognition -The automated process of validating a claimed identity based on the image of a face. BioStar extracts and analyzes the facial features such as the skin texture and the shapes of the face, eyes, nose and mouth from a captured face image and compares them with those of all the registered persons.

false acceptance rate: The false acceptance rate (FAR) is a measure of the likelihood that a biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances to the number of identification attempts.

false rejection rate: The false rejection rate (FRR) is a measure of the likelihood that a biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR is typically stated as the ratio of the number of false rejections to the number of identification attempts.

fingerprint recognition -The automated process of matching two human fingerprints: one previously recorded and one being provided by a user for authentication. BioStar incorporates Suprema's award-winning algorithms for recognizing fingerprints.

fingerprint sensor: A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for fingerprint recognition.

fire alarm zone: A zone that is used to interface with fire alarms and control doors when a fire is detected.

Glossary

host: A host is the device that serves as the master in a RS485 network. The host device relays data packets between external devices (or a larger network) and slave devices connected to the RS485 network.

input signal: The signal sent to a device by an external object, such as an exit button.

operator: Operators are personnel who have rights to use BioStar clients. BioStar includes three pre-defined classes for operators: administrators, operators, and managers. BioStar also supports a maximum of 16 custom operator classes.

output signal: The signal sent to an external device, such as an alarm siren or electronic door strike.

proximity card: Proximity cards (or "prox" cards) are contactless integrated circuit devices used for security access. BioStation, BioEntry Plus, and BioLite Net devices support EM4100 cards; BioStation Mifare, BioEntry Plus Mifare, BioEntry W Mifare and BioLite Net, and DStation devices support MIFARE and iCLASS cards; and BioStation HID and BioEntry Plus HID devices support HID proximity cards.

RF device: Short-range radio frequency devices used to gain access to doors. The BioStar system allows 3rd party RF devices to be added to the system to incorporate existing hardware into the access control configuration

security level: see: *false acceptance rate*.

time and attendance (T&A): This designation refers to the processes and functions that monitor and report check-in and check-out activities by employees and allow administrators to define time slots and schedules. The information collected by the BioStar system can be used in conjunction with external systems for time reporting and payroll capabilities.

timed anti-passback: A security protocol that prevents reauthorization of a user for a specified period of time. See also: *anti-passback.*

timezone: A customizable schedule that can be used to allow or restrict access during specified hours. Timezones can combined with doors to create access groups.

user: A user is any person who has access rights. A user's access rights are comprised of individual rights (user level), membership in access groups, and time restrictions.

Wiegand interface: The Wiegand interface is a wiring standard used to connect a card swipe mechanism to the rest of an electronic entry system. The interface uses three wires, one of which is a common ground and two of which are data transmission wires usually called DATA0 and DATA1, but sometimes also labeled Data High and Data Low.

zone: A zone consists of two or more devices that are grouped together. BioStar includes seven types of zone classifications.

Index

Index

Index

Index

Index

Index

W

X

Z

suprema

Suprema Inc.

16F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi,
463-863 Korea

Tel: +82-31-783-4502 **Fax**: +82-31-783-4503

Email: sales@supremainc.com **Homepage**: www.supremainc.com