suprema
BioStar

BioStar 1.2 Administrator Guide

suprema

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

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, life saving, 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

BioStar V1.2 supports the following devices:

- **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.

- **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.

- **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.

- **BioMini** - The BioMini device is a fingerprint scanner that can be used for convenient user enrollment. Installing the device is simple: plug it into a USB connection on any computer that is connected to the BioStar server and install a driver.

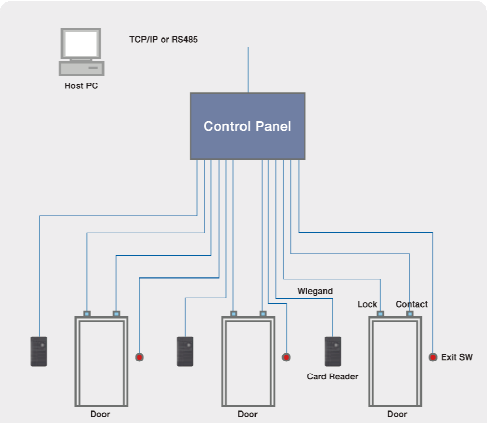
- **Secure I/O** - The Secure I/O device provides a convenient way to increase the security of externally mounted devices or expand the capabilities of your system. When doors are controlled by a secure I/O device, intruders cannot open doors even if they succeed in uninstalling external devices. To 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.

1.1 Logical Configuration

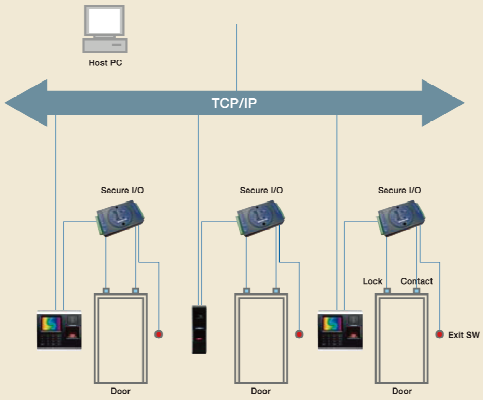
BioStar is a distributed intelligence system. Instead of the complex wiring and centralized control required by conventional access control systems, Suprema's access control devices can be connected via TCP/IP or wirelessly to a local area network or connected directly via serial connections. User information, 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 or BioEntry Plus 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.



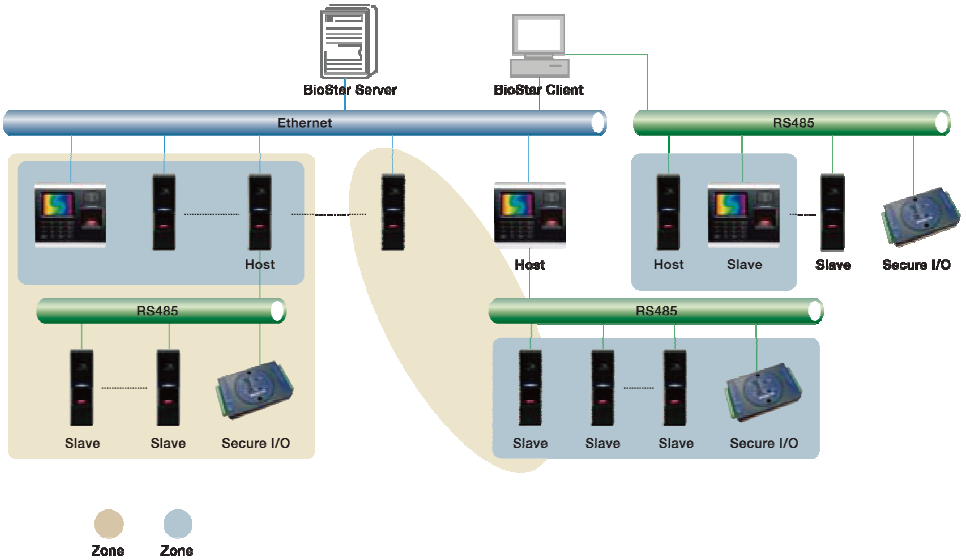
Conventional Centralized Access Control Systems



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. When used with the numerical keypads on BioStation terminals, 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.

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 3.5.2.

BioStar also provides administrators with the ability to read EM4100 and HID proximity cards and read, issue, and format MIFARE® access cards. For more information about access cards, see section 3.5.3.

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 BioStation, BioEntry Plus, or BioLite Net 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, and 4.4.

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 3.7.

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 devices and event settings for BioEntry Plus 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 4.6.

1.2.5 Door 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 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 and 4.3.

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 3.4.

1.2.7 Time and Attendance

BioStar V1.2 includes 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 devices and 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 3.8 and 4.5.

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 a BioStar express installer, a BioStar server installer, and a BioStar client installer. The express 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 (32-bit versions only):

- Windows Vista
- Windows XP, Service Pack 1 or later
- Windows 2003
- Windows 2000, Service Pack 4 or later

2. Install the BioStar Software

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

- CPU - Intel Pentium or similar processor, capable of processing speeds of 1GHz or faster
- RAM - 512MB
- HDD - 5GB

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

- CPU - Intel Pentium Dual Core or similar processor, capable of processing speeds of 2GHz or faster
- RAM - 1GB for Windows XP; 2GB for other operating systems
- HDD - 10GB

2.2 Run the BioStar Express Installer

You should run the BioStar express 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 6 of section 2.3.

The express installer will install the following components:

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

Before you run the BioStar express 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 express installer,

1. Insert the BioStar installation CD into a compatible media drive.
2. Locate the installation directory and run BioStar 1.2 Express Setup.
3. Follow the on-screen prompts to begin the installation.

2.3 Install the BioStar Server Application

If you do not choose to use the express installer, you must install the BioStar server and client applications separately. 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.

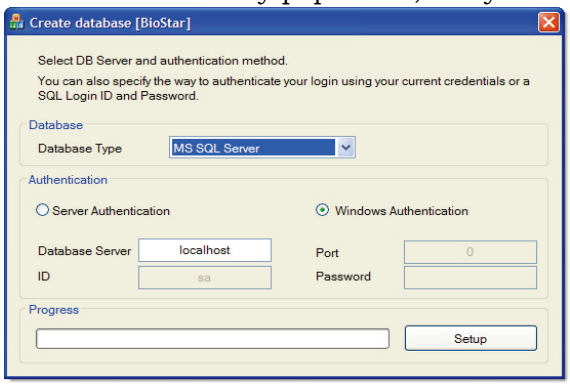
The BioStar server installer will add the following components to your system:

- BioStar server application
- MS SQL Server Express (optional)
- Auxiliary libraries - OpenSSL and Microsoft Visual C++ 2005 Redistributable
- 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 1.2 Server Setup.
3. Follow the on-screen prompts to begin the installation.
4. During the installation, you will be required to accept the OpenSSL license agreement and select a destination folder for the OpenSSL program files.
5. You will also be asked whether or not you wish to install the MS SQL Server Express edition. If you will use a pre-installed version of MS SQL Server or MySQL, you may click No when this message appears. If you decide to use the express edition in this step, you can skip to step 7. The database setup process will be automated when you install the express edition.

6. When the Create Database [BioStar] window appears, select a database type (MS SQL Server or MySQL). The database server address and port numbers will be automatically populated, but you should verify that they are correct.



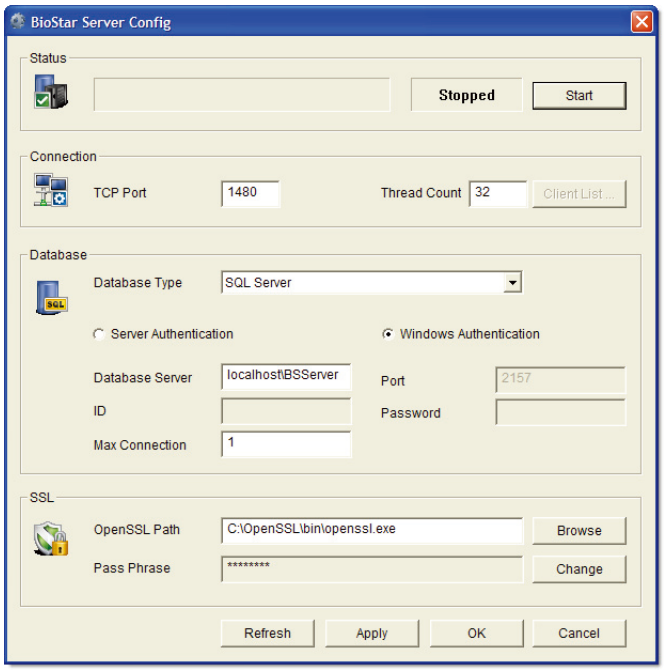
7. If you choose MS SQL Server, you must configure the authentication method as well (MySQL allows only server authentication):
   - **Server authentication** - this option uses login IDs and passwords to authenticate users that are created by and stored on the SQL Server. These credentials are not based 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.
8. Click **Setup** to create the SQL database.
9. When the SQL database setup is complete, click **Finish**.
10. The setup program will perform a few remaining processes before the server installation is complete. Click **Finish**.

2.3.1 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.

To open the server configuration utility, locate and run the BSServerConfig.exe file. By default, a shortcut to this utility will be added to the desktop during installation of the BioStar server. You may also locate this file inside the "Server" folder where the BioStar application was installed.



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. In most cases, you can use the default port (1480).

- **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.

- **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.

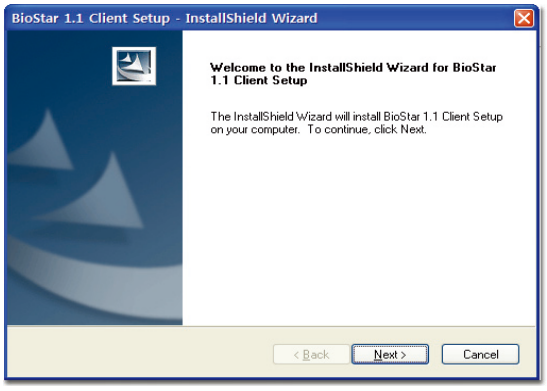
2.4 Install the BioStar Client Application

Before you install the BioStar client application, close all other running applications. The client application installer will add the following components to your system:

- BioStar client application
- Auxiliary libraries - OpenSSL and Microsoft Visual C++ 2005 Redistributable

To install BioStar client application,

1. Insert the BioStar installation CD into a compatible media drive.
2. Run BioStar 1.2 Client Setup to launch the installation wizard.



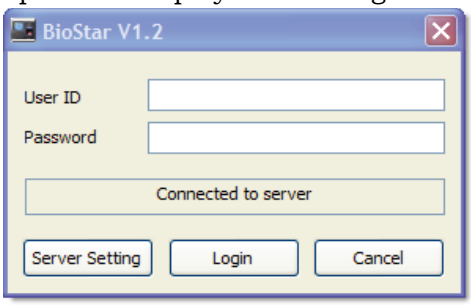
3. Follow the on-screen prompts to install the BioStar Client.

2.4.1 Log in to BioStar for the First Time

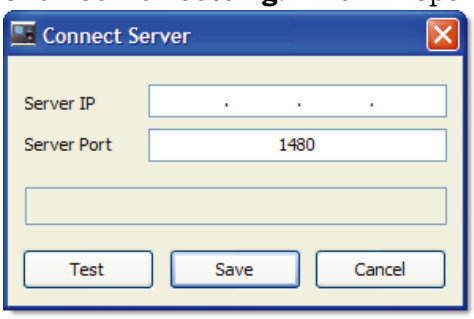
If you restarted the system after installation, the BioStar server should run automatically in the background. If you have not restarted the system, you may be required to manually connect to the server before proceeding (see section 2.3.1). When logging in to BioStar for the first time, you will be 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 window will open automatically. In this case, skip to step 6. If BioStar cannot connect to the server, the Login window will open and display the message “Cannot connect to server.”

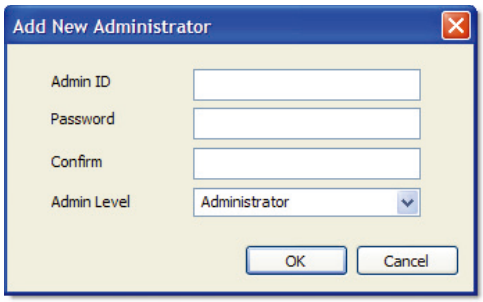


2. Click **Server Setting**. This will open the “Connect Server” window.



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 window.



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 window.
8. Enter a User ID and password and click **Login**.

2.5 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.

2.5.1 Change the Theme

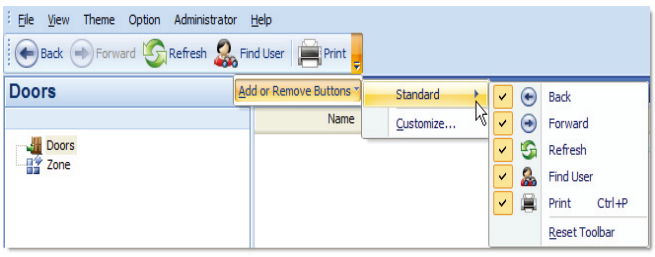
The BioStar interface includes two preset themes based on MS Office styles:

- Office 2003
- Office 2007

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

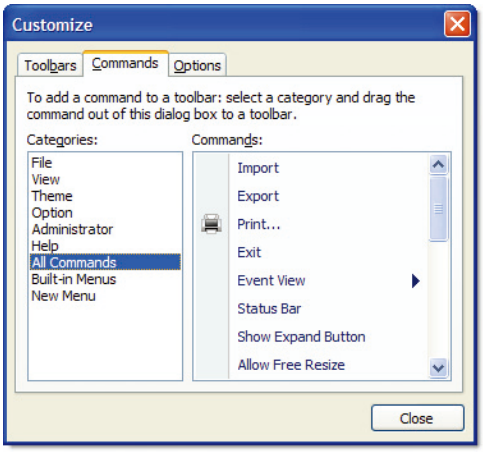
2.5.2 Customize the Toolbar

The BioStar interface includes a standard toolbar near the top left of the window. 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 window.
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.

2.5.3 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,

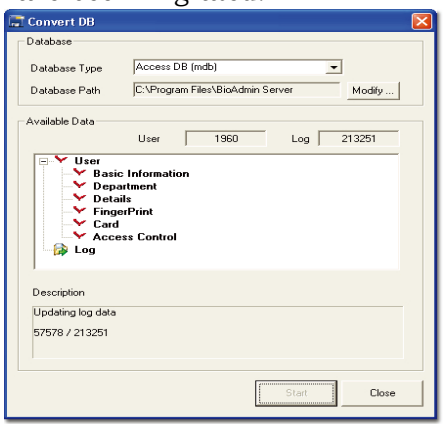
1. From the menu bar, click **View > Event View**.
2. Click type of event view to change (*User* or *Doors/Zone*).
3. Click a default event period (*1 day*, *3 day*, or *7 day*).

2.6 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*. By default, this tool will be installed in the same folder as the BioStar software.
2. Click **Yes** to acknowledge the warning dialogue that appears to remind you that identical information in BioStar will be overwritten.
3. In case of already installed, click **Start** to begin the migration. When the process is complete, the Convert DB window 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 Administration Concepts

BioStar allows for multiple levels of administration, operation, and interaction with the system. Administrators are capable of adding and configuring devices, users, doors, zones, and access groups. In addition, administrators can grant various privileges to operators, users, and other administrators. BioStar also allows for the creation of custom administration roles.

BioStar is a server-client application that can be monitored and managed by operators who may access the BioStar server via a remote client terminal. Operators can be granted various privileges by administrators, other than the privilege to create and delete other administrator or operator accounts.

As of version 1.2, BioStar allows administrators and operators to 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 can view T&A reports for all users and users can view reports of their own T&A activities.

Although your administration requirements may vary, 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.

Below the operator level, managers can be granted privileges to read information about users. Depending on your organization's requirements, the capability to view events may be useful for other management purposes.

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 2.3.1). 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

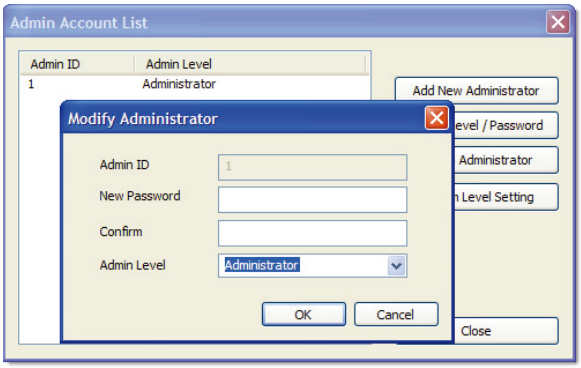
To add an administrative account,

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



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.

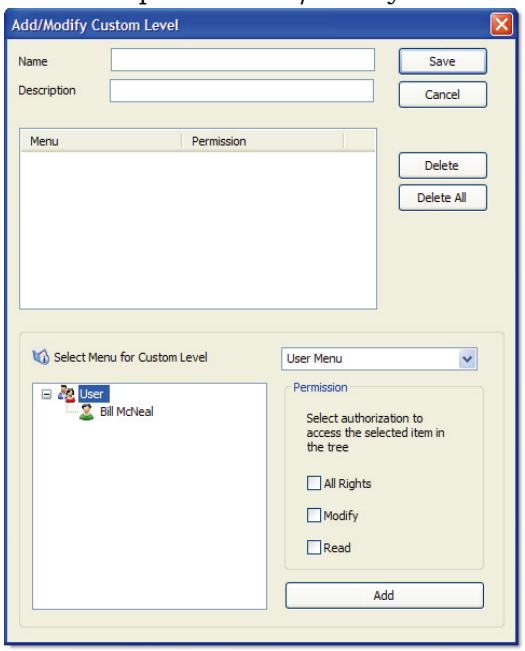
3.1.2.3 Create a custom administration level

If you have the need to define a specific administrator role, you can do so by creating a custom administrator level. When creating a custom administrator level, you can specify permissions (All Rights, Modify, or Read) for items in each of the shortcut menus. Custom administrator levels that you create will be selectable from the Admin Level drop-down in the Add New Administrator window.

To create a custom administrator level,

1. From the menu bar, click **Administrator > Admin Account** to open the Admin Account List window.
2. Click **Custom Level Setting**.

3. From the Custom Level List window, click **Add Custom Level**. This will open the Add/Modify Custom Level window.



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. Select a permission level by clicking the checkbox next to an option.
8. Click **Add** to include the permission in the custom level.
9. Repeat steps 6-8 as necessary to add other permissions.
10. When you are finished customizing the level, click **Save**.

You can now create new administrative accounts for any of the custom 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 3.9.3 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,

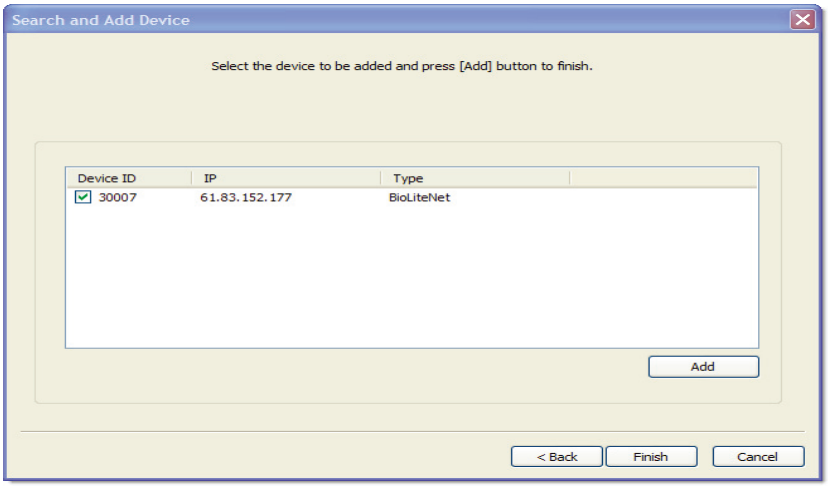
1. Click **Device** in the shortcut pane.
2. In the Task pane, click *Add Device*.
3. When the wizard appears, click the radio button next to a connection type:
   - **LAN** - Choose this option to search for devices connected via Ethernet or Wireless LAN.
   - **Serial** - Choose this option to search 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.
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: 1470, BioEntry Plus/BioLite Net: 1471, 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.
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. 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.

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.

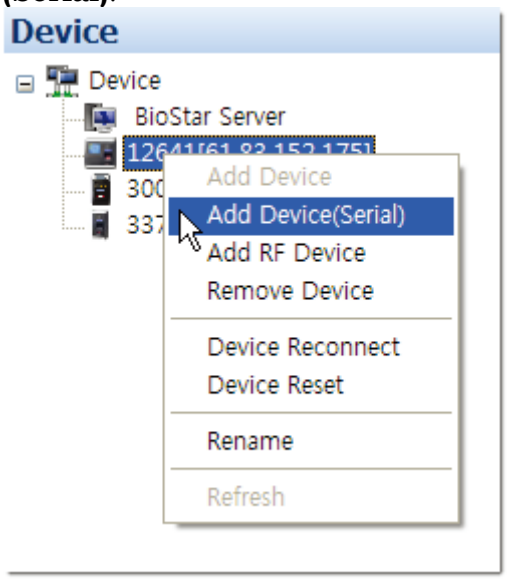
If your configuration includes slave devices, you must perform an additional search to locate and add those devices.

First, configure the host device:

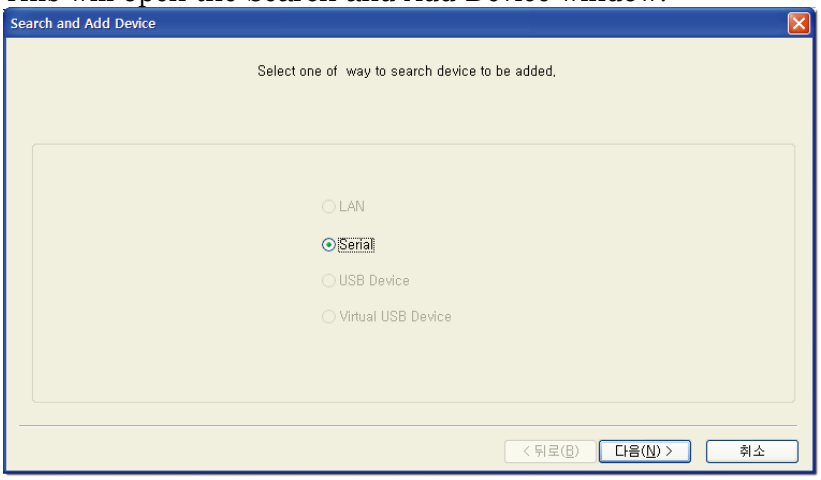
1. Search for and add the host device as described in section 3.2.1.
2. Click **Device** in the shortcut pane.
3. In the navigation pane, click the host device.
4. In the device pane, click the Network tab.
5. Change the RS485 serial setting by selecting *Host* from the Mode drop-down list.
6. Click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



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.

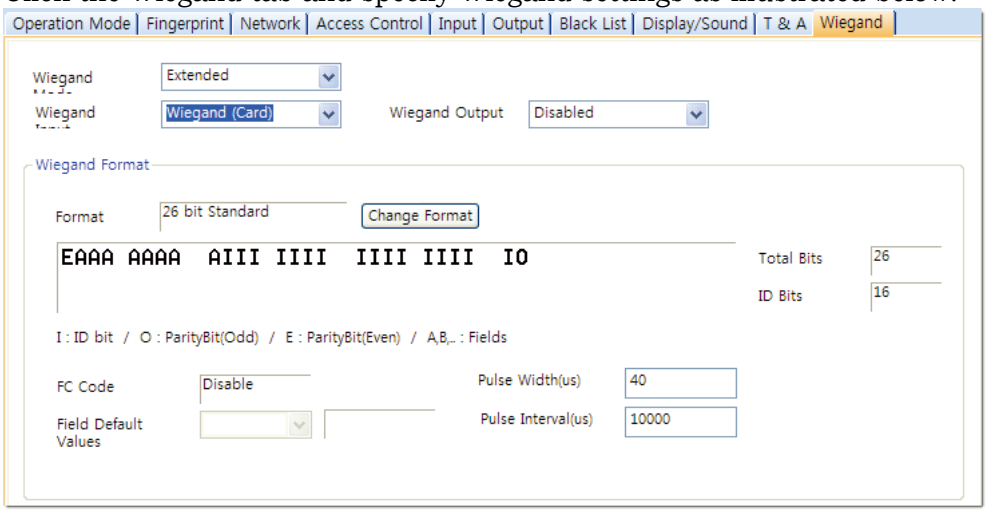
3.2.3 Add an RF Device

Before BioStar 1.2, 3rd party RF devices have been connected to Suprema devices (BioStation, BioEntry Plus, and BioLite Net devices) and functioned only as physical extension of the Suprema devices. As of BioStar 1.2, however, 3rd party RF devices can be connected to Suprema devices and function as independent devices so that you can associate them with doors and can also include them in zones.

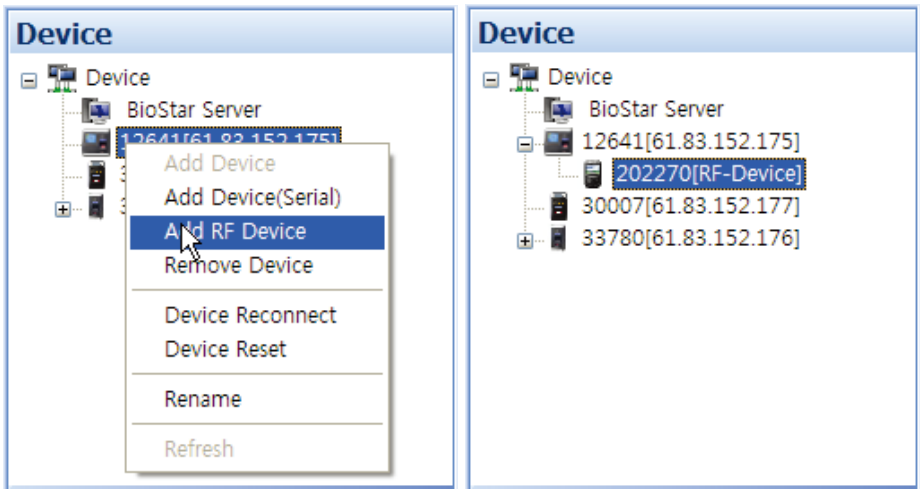
To add an RF device,

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 illustrated below.



   a. Select **Extended** in the Wiegand Mode drop-down list.
   b. Select **Wiegand (Card)** in the Wiegand Input drop-down list.
   c. 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*.

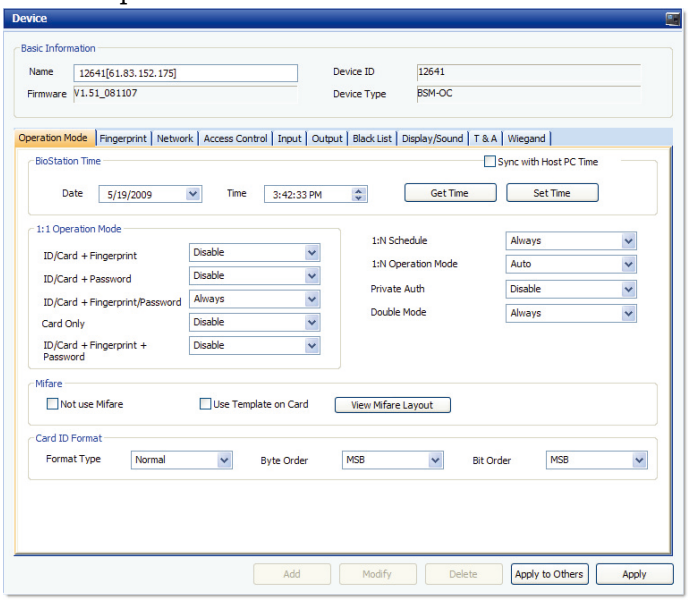


Note: For more information about using your 3rd party RF devices, consult the user guidance for the RF device.
And Wiegand format should be configured properly in Suprema device for it to work compatibly with 3rd party RF devices.

3.2.4 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, 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 disable MIFARE card access on BioStation Mifare devices.

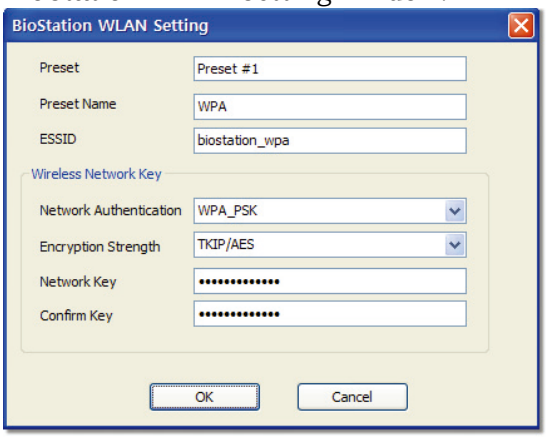
- **Display/Sound** - Use this tab to adjust display or sound settings and add background images and sounds.
- **T&A** - Use this tab to configure time and attendance settings.
- **Wiegand** - Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.7.

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 window.

3.2.4.1 Connect a BioStation device via wireless LAN

Certain BioStation devices support wireless LAN connections. To configure the settings for a wireless LAN connection,

1. Click **Device** in the shortcut pane.
2. Click a BioStation 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. This will open the BioStation WLAN Setting window.



7. Configure the following settings:
   - **Preset Name** - enter a name for the configuration that will appear on the BioStation device connected via WLAN.
   - **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.

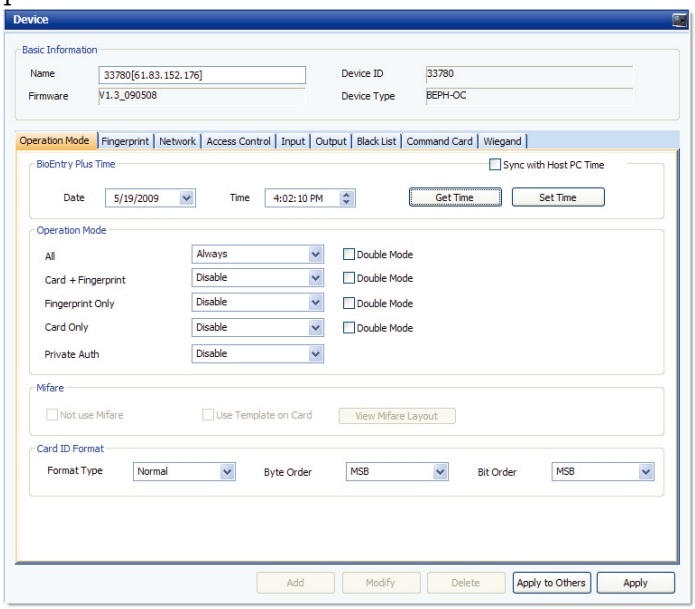
- **Encryption Strength** - select an encryption strength from the drop-down list (available options depend on network authentication setting).
- **Network Key** - enter the network key.
- **Confirm Key** - re-enter the network key.

8. Click **OK** to save your changes.

3.2.5 Configure a BioEntry Plus Device

To configure a BioEntry Plus 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.

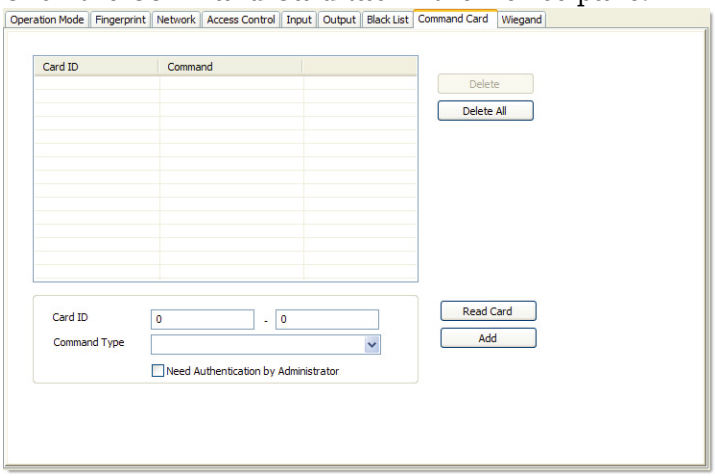
- **Input** - Use this tab to add or modify inputs to the device.
- Output - Use this tab to add or modify outputs from the device.
- **Black List** - Use this tab to disable MIFARE card access on BioEntry Plus Mifare devices.
- **Command Card** - Use this tab to issue command cards that can control BioEntry Plus devices. For more information about issuing command cards, see section 3.2.5.1.
- **Wiegand** - Use this tab to configure the Wiegand format. For more information about Wiegand formats, see section 3.2.7.

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 window.

3.2.5.1 Issue command cards

Command cards allow you to enroll and delete users directly from a BioEntry Plus device. To issue command cards,

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

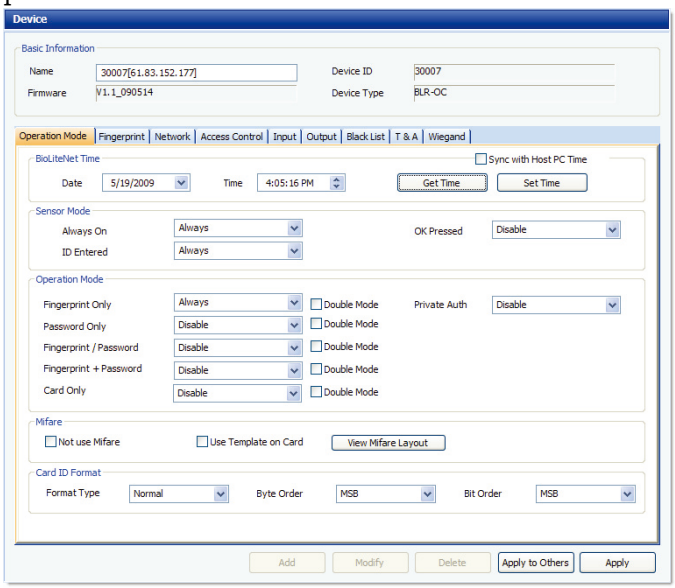


4. Click **Read Card**.
5. Place a command card on the device.
6. Select a command type from the drop-down list.
7. If desired, set the command card to require administrator authentication by clicking the checkbox next to the option.
8. Click **Add**.

3.2.6 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:



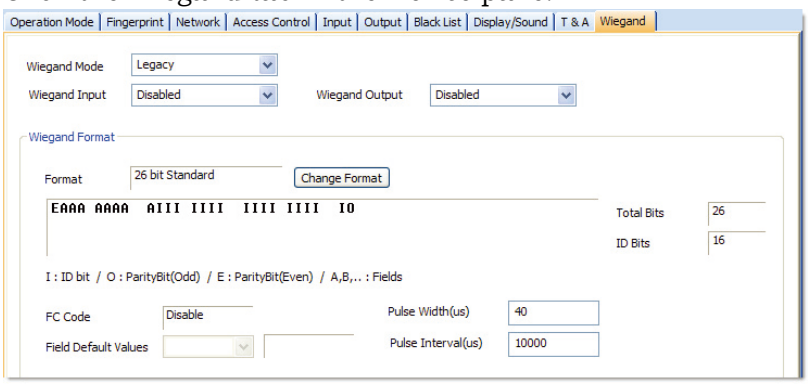
3. Configure device information on the following tabs. For an explanation of device settings, see section 5.1.2.
   - **Operation mode** - Use this tab to set the device time or retrieve it from a host PC, adjust settings for operation modes, and adjust options for fingerprint recognition.
   - **Fingerprint** - 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 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 disable MIFARE card access on BioLite Net Mifare devices.
   - **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 3.2.7.

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 window, and click **Apply**.

3.2.7 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.



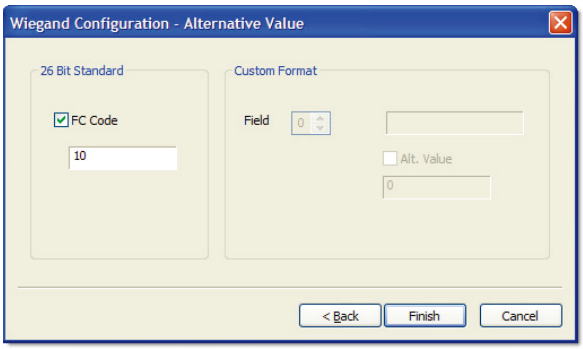
4. Click **Change Format**. This will open the Wiegand Configuration wizard.
5. Click a radio button to select one of the following formats:
   - **26-bit Standard** - this format is the most widely used and consists of an 8-bit FC code and a 16-bit ID. You cannot change the bit definition of the format 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.
   - **Custom** - with a custom format, you can define the ID bits, parity bits, and alternative values. During verification, the device will first check the parity of an input string. If the parity is correct, the device will check the ID. Only when all verification has been completed will the device send an output string, which can also be customized to differ from the input string.

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.

3.2.7.1 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 window.

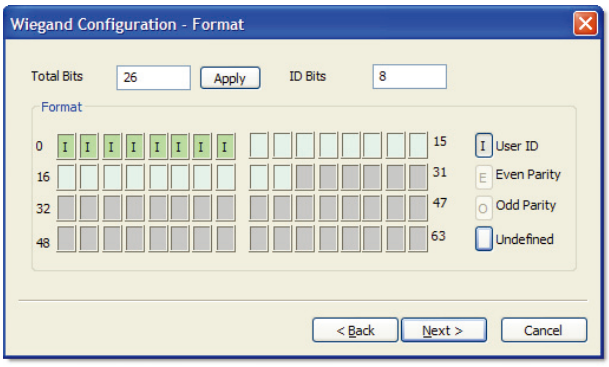


2. Click the FC Code checkbox and enter a new FC Code.
3. Click **Finish** to close the wizard.

3.2.7.2 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 Format window.



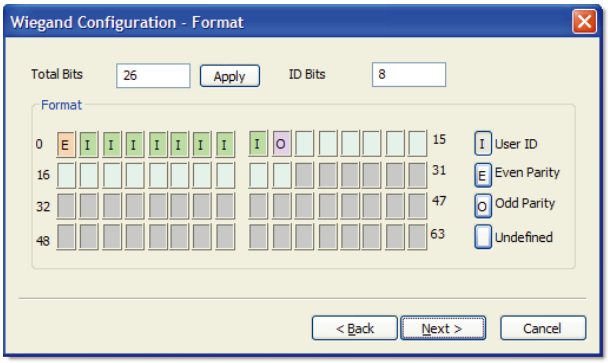
2. If desired, enter a new total number of bits and click **Apply**.
3. Click the User ID button (I) on the right.
4. Assign ID bits by clicking the appropriate squares.

5. Click Next until you reach the Alternative Value window.
6. Click **Finish** to close the wizard.

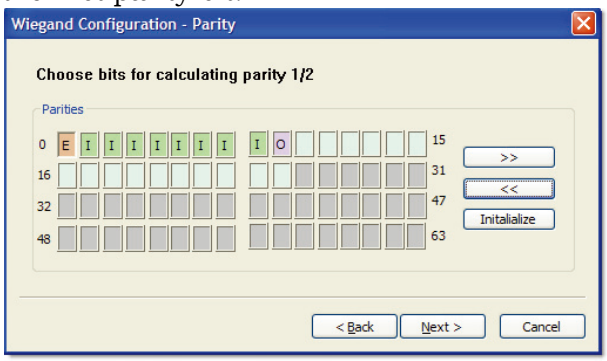
3.2.7.3 Configure a custom Wiegand format

When you select a custom format, you can customize the total number of bits, assign ID bits, define parity bits, and set alternate values for the output string.

1. After selecting the format in the wizard, click **Next** to advance to the Format window.



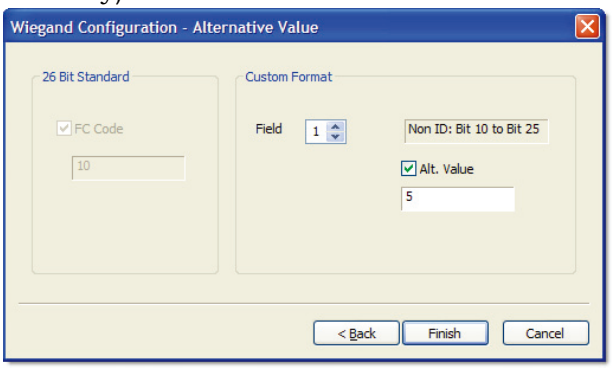
2. If desired, enter a new total number of bits and click **Apply**.
3. Click the User ID button (I) on the right and assign ID bits by clicking the appropriate squares.
4. Click the Even Parity button (E) on the right and assign an even parity bit by clicking on the appropriate squares.
5. Click the Odd Parity button (O) on the right and assign an odd parity bit by clicking on the appropriate squares.
6. Click **Next**.
7. In the Parity window, select the bits that will be used to calculate the first parity bit.



8. 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.

9. Click **Next**.
10. In the Alternative Value window, select a field to customize (non-ID bits only).



11. Click the Alt Value checkbox and enter a new value for the output string.
12. Repeat steps 10-11 as necessary to customize the rest of the output string.
13. 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.

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*.
4. Right-click *New Door*, click *Rename*, and type a name for the door.

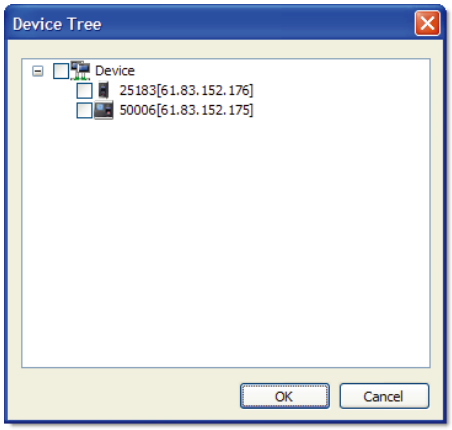
3.3.2 Associate a Device With a Door

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*.

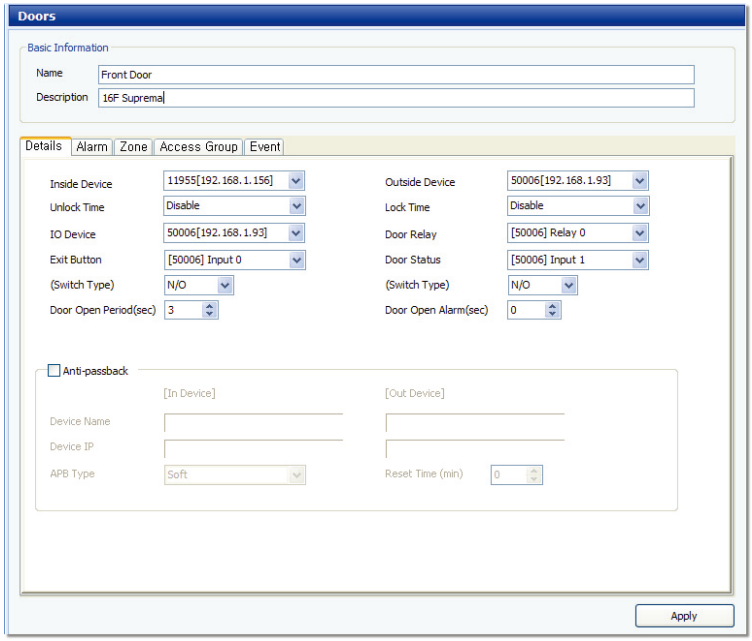
3. Select a device from the Device Tree window by clicking the checkbox next to a device name.



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 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.

3.4.1 Determine Which Zones to Use

In total, the BioStar system supports five 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 3.4.2.4, 3.4.2.5, 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.

3.4.2 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.

3.4.2.1 Add a zone

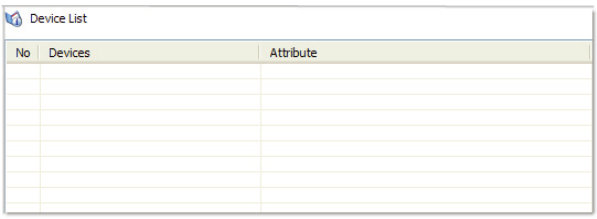
To add a new zone,

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 3.4.1 for zone descriptions).
6. Press **OK**.

The Zone pane will appear on the right side of the window.

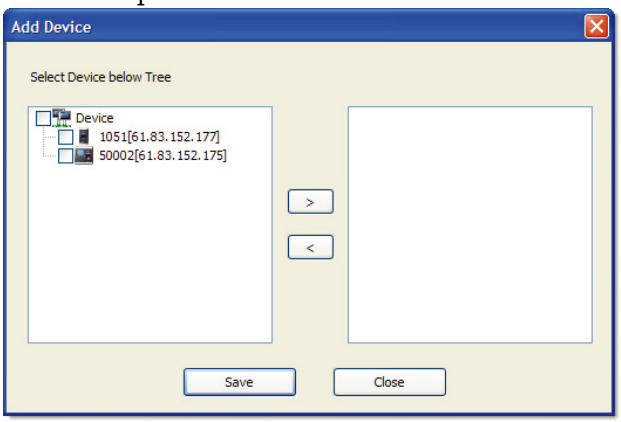
3.4.2.2 Add a device to a zone

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).



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 Devices window.

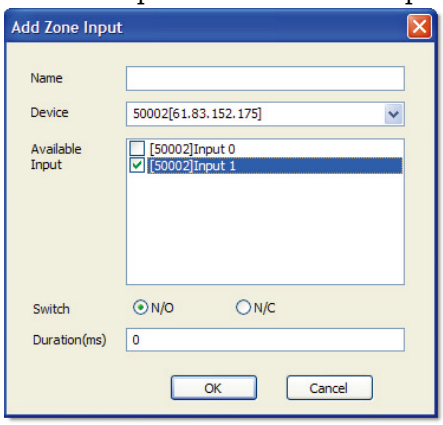


4. Select a device (or multiple devices) from the list and click **>**.
   - **Anti-passback zones** - when the Select Zone Attribute pop-up appears, select an attribute from the drop-down list (*In Device* or *Out Device*).
   - **Alarm zones** - when the Select Zone Attribute/Type pop-up appears, select 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* radio button to specify how to arm or disarm zones, and then press **OK**. For more information about arming or disarming zones, see section 3.4.2.5.
5. Press **Save** to add the devices to the list.

3.4.2.3 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 Inputs window.



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.

3.4.2.4 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 3.4.2.5 and 3.9.

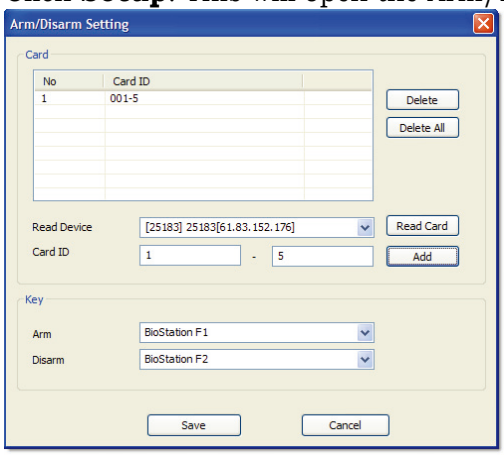
- **Program Sound** - set a sound to be emitted by the software (at the host computer or BioStar Server). To add custom sounds, see section 3.9.1.2.
- **Device Sound** - set a sound to be emitted by a particular device.
- **Send Email** - create an email alert to send when an alarm is activated and select recipients or email alerts. For more information about email alerts, see section 3.9.2.

- **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.

3.4.2.5 Configure arm and disarm settings

After adding an alarm zone, you can configure the actions that will arm and disarm the 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. If necessary, expand the Zone tree first.
3. Click the Details tab in the Zone pane.
4. Click **Setup**. This will open the Arm/Disarm Setting window.



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 **Save**.

3.4.2.6 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, click the checkbox next to a group name and then click **Apply**.

3.4.2.7 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.

3.5 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 or BioLite Net devices can be used for fingerprint scanning when networked to the BioStar server or the SFR300 USB device can be connected directly to a BioStar client to provide convenient fingerprint scanning at a registration location.

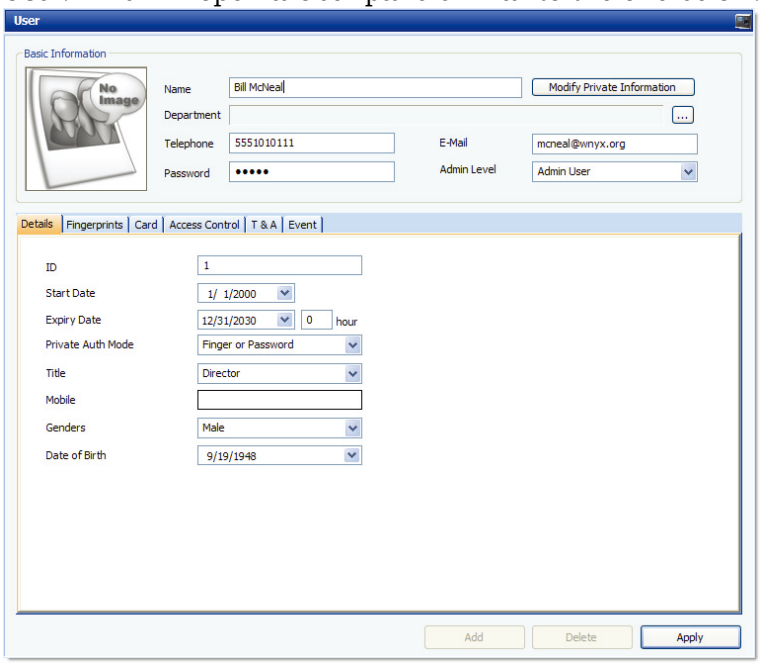
When adding users, you will first need to create a user account. Once the account has been created, you can register fingerprints and access cards or edit user details as desired.

3.5.1 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, see section 3.5.4.3. To migrate user data from an existing BioAdmin database, see section 2.4.

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.
   - **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.

- **Genders** - 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 3.5.2) and access cards (see section 3.5.3) as necessary.
5. When you are finished adding details to the user's account, click **Apply**.

3.5.2 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.

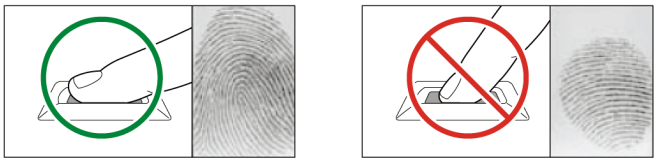
When registering fingerprints, keep the following tips in mind:

- 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.

3.5.2.1 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.



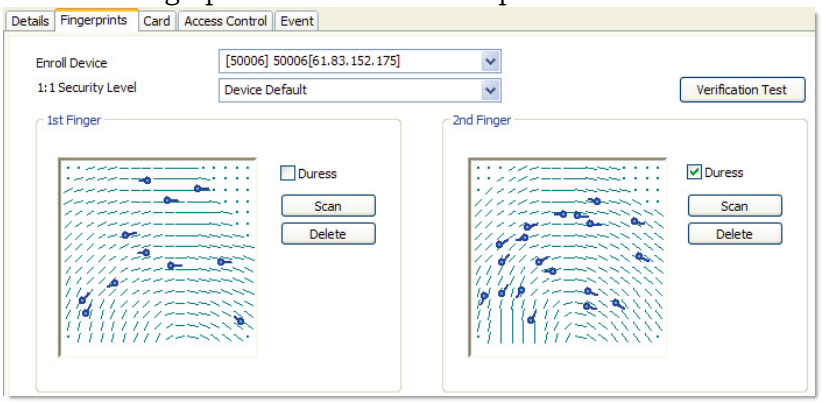
3.5.2.2 Register fingerprints

BioStar allows you to register up to two fingerprints per user. If desired, one of the fingerprint scans 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 enrollment device you will use for scanning fingerprints from the drop-down list.
5. Select a security level from the next drop-down list.

6. In the 1st Finger section, press **Scan**, and then have the user place his or her finger on the scanner twice, as prompted by the BioStar interface.
7. If desired, click the checkbox next to the Duress option to set this fingerprint as the duress signal.
8. Repeat steps 5-7 in the 2nd Finger section to register a second fingerprint.
9. Click **Apply** to save your changes.

3.5.2.3 Enroll users via command cards

After issuing command cards, you can enroll users directly from a BioEntry Plus device. For more information about issuing command cards, see section 3.2.5.1. To enroll a user on a BioEntry Plus device via a command card,

1. Place an enroll card on a BioEntry Plus 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 a 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).

3.5.3 Issue Access Cards

Suprema manufactures access control devices that support multiple types of access cards: EM4100, HID proximity, and MIFARE® cards. BioStation, BioEntry Plus and BioLite Net devices support EM4100 cards, BioStation Mifare, BioEntry Plus Mifare and BioLite Net devices support MIFARE cards, and BioStation HID devices support HID proximity cards.

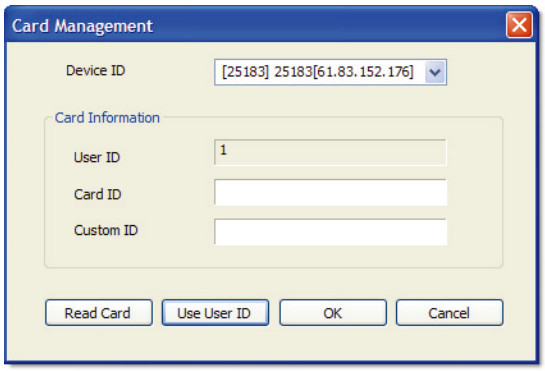
EM4100 and HID cards require only a card ID to complete card registration, while MIFARE cards support two operation modes: Card Serial Number (CSN) and Template-on-Card modes. When using the CSN mode, you can read the serial number just as you would for an EM4100 or HID card. When using Template-on-Card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

3.5.3.1 Issue EM4100 cards

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 a “EM4100” from the Card Type drop-down list.
5. Click **Card Management**. This will open the Card Management window.

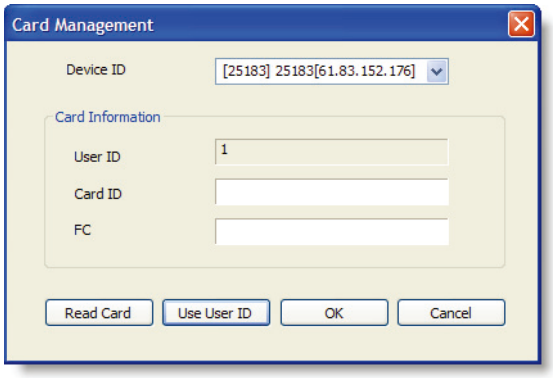


6. Select a Device ID from the drop-down list.
7. Enter a card ID (32 bits) and custom ID (8 bits) either manually or by reading from the card (you can also click **Use User ID** to insert the user’s ID in these fields):
   - To enter the data manually, type the card ID and custom ID in the corresponding 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.

3.5.3.2 Issue HID proximity cards

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 “HID Prox” from the Card Type drop-down list.
5. Click **Card Management**. This will open the Card Management window.

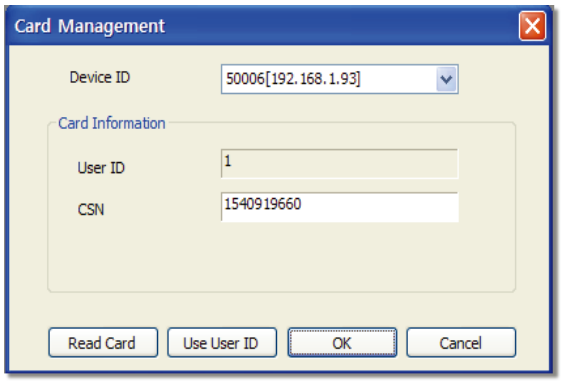


6. Select a Device ID from the drop-down list.
7. Enter a card ID and facility code (FC) either manually or by reading from the card (you can also click **Use User ID** to insert the user’s ID in these fields):
   - To enter the data manually, type the ID and facility code in the corresponding fields, 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.

3.5.3.3 Issue MIFARE CSN cards

MIFARE 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” from the Card Type drop-down list.
5. Click **Card Management**. This will open the Card Management window.

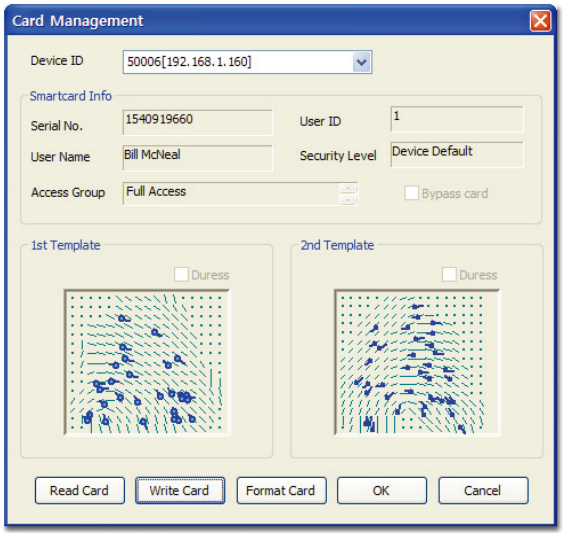


6. Select a Device ID from the drop-down list.
7. Enter a card ID either manually or by reading from the card (you can also click **Use User ID** to insert the user’s ID in these fields):
   - To enter the data manually, type the ID and facility code in the corresponding fields, click OK, and then skip 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.

3.5.3.4 Issue MIFARE template cards

MIFARE template cards allow you to store user information and fingerprint templates directly on the card. 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 Template” from the drop-down list.
5. Click **Card Management**. This will open the Card Management window.



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.

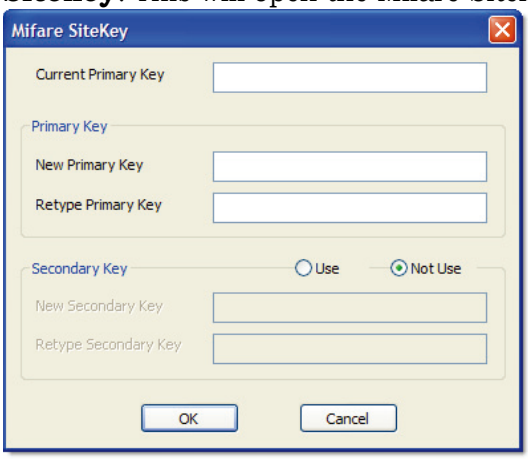
3.5.3.5 Change the MIFARE site key

Data encryption for MIFARE 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 site keys (primary and secondary), so that you can change the site key for existing cards.

Note: Site keys must be carefully guarded. If the site key is revealed, your security system can be bypassed.

To change the MIFARE site key,

1. From the menu bar, click **Option > Mifare Card > Mifare Sitekey**. This will open the Mifare Sitekey window.



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* radio 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.

3.5.3.6 Edit the MIFARE layout

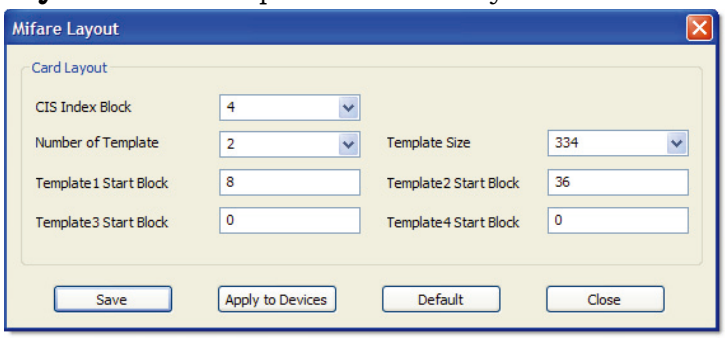
BioStar allows you to customize the MIFARE layout that is used to record user information and fingerprint templates. This layout will be applied to all new MIFARE cards issued with the devices you specify (BioStation Mifare, BioEntry Plus Mifare or BioLite Net devices).

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 > Mifare Card > Mifare Layout**. This will open the Mifare Layout window.



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 window.
4. To save your changes, click **Save**.
   Note: To reset any changes you have made, click **Default**. To exit the window without saving changes, click **Close**.

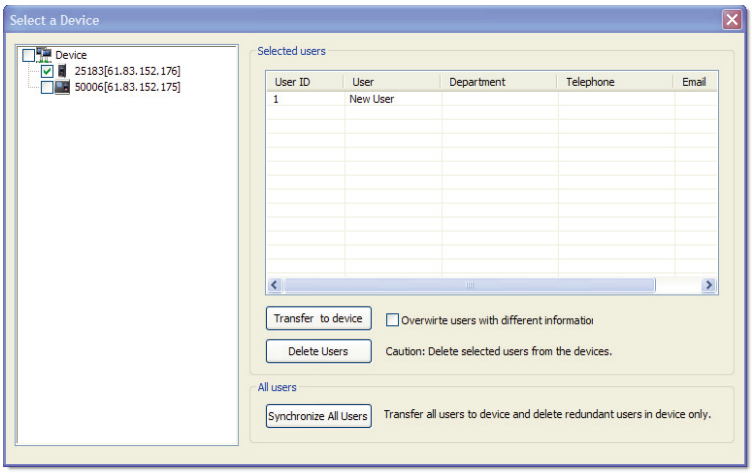
3.5.4 Transfer User Data

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.

3.5.4.1 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 window.



3. Select a device or devices from the list on the left by clicking the checkboxes next to device names.
4. Click a user name (you can hold down the Ctrl key while selecting multiple users).
5. If desired, click the checkbox to overwrite users with different information.
6. 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**.

3.5.4.2 Synchronize all users

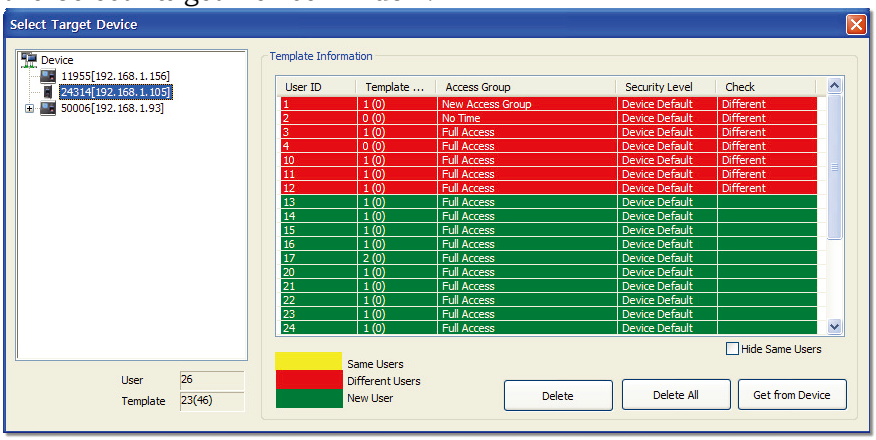
To synchronize all user information between the BioStar server and connected devices,

1. Click **User** in the shortcut pane.
2. In the task pane, click *Transfer Users to Device*. This will open the Select a Device window (see section 3.5.4.1).
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**.

3.5.4.3 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 window.



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).

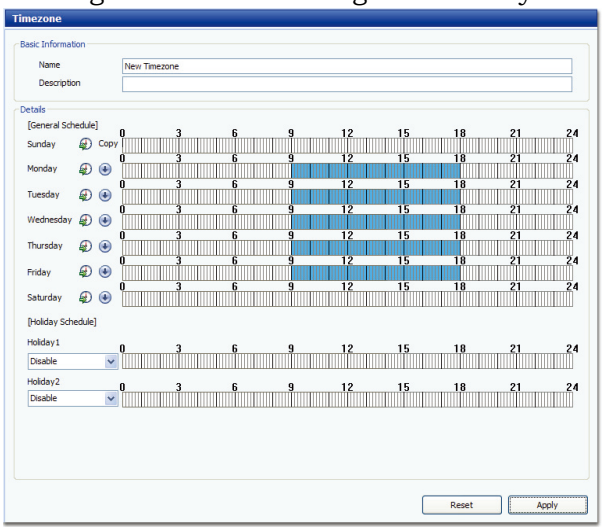
3.6 Setup Timezones

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 3.7).

3.6.1 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.



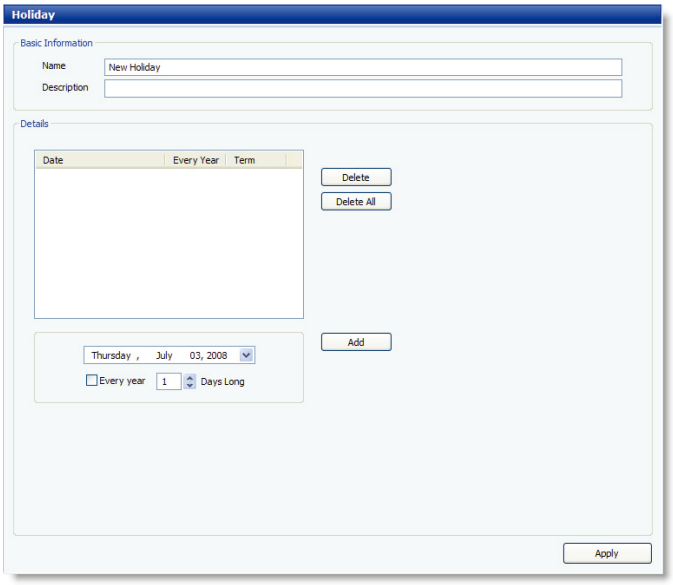
5. If desired, you can add up to two holiday schedules to the timezone. To create holiday schedules, see section 3.6.2.
6. When you are finished creating the timezone, click **Apply**.
7. Next, transfer the timezone data to devices:
   a. In the task pane, click *Transfer to Device*. This will open the device tree window.
   b. Select a device or devices by clicking the checkboxes in the device tree.
   c. Click **OK**.

You can now combine the timezone with door permissions to create an access group (see section 3.7).

3.6.2 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.



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

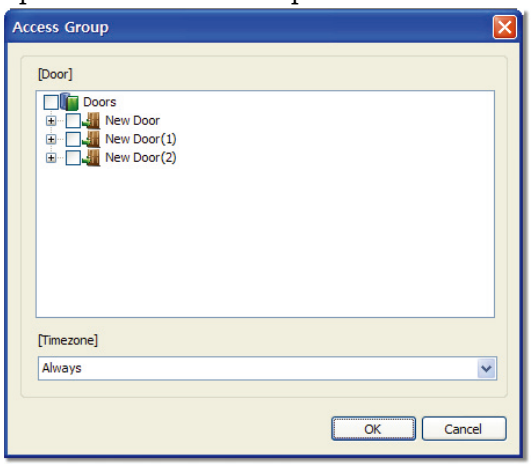
3.7 Setup Access Groups

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 3.6). After creating access groups, you must manually transfer the data to affected devices (see section 3.7.4).

3.7.1 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 window.



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 window.
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.

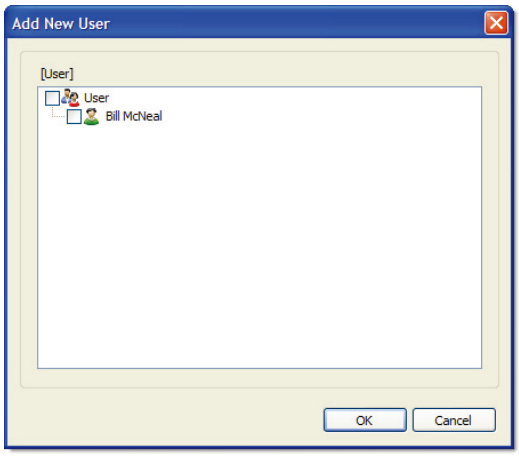
3.7.2 Add Users to Access Groups

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 3.7.3. 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 window, select users to add to the group by checking user groups or individual users.



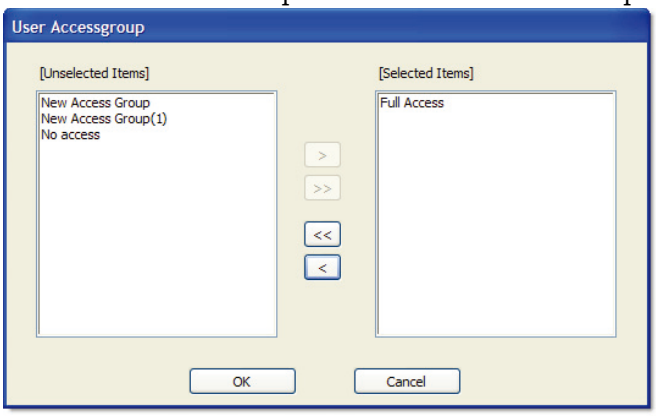
4. Click **OK**.

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

3.7.3 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 window.



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**.

3.7.4 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 window.
3. Select a device or devices by clicking the checkboxes in the device tree.
4. Click **OK**.

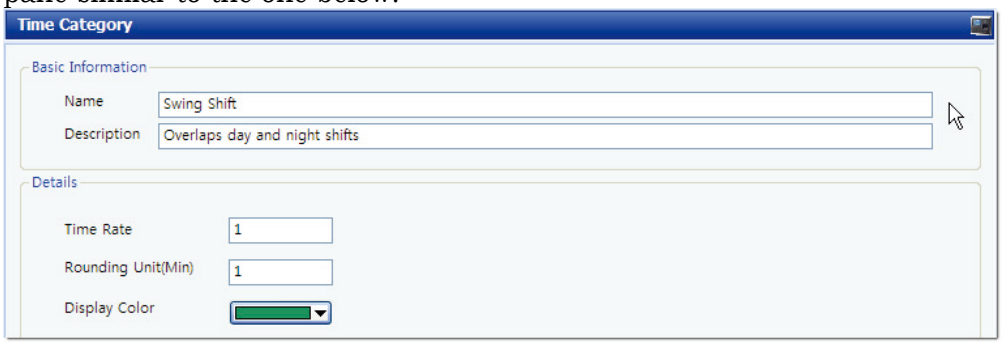
3.8 Setup Time and Attendance

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 3.6.2 to configure time and attendance options.

3.8.1 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.

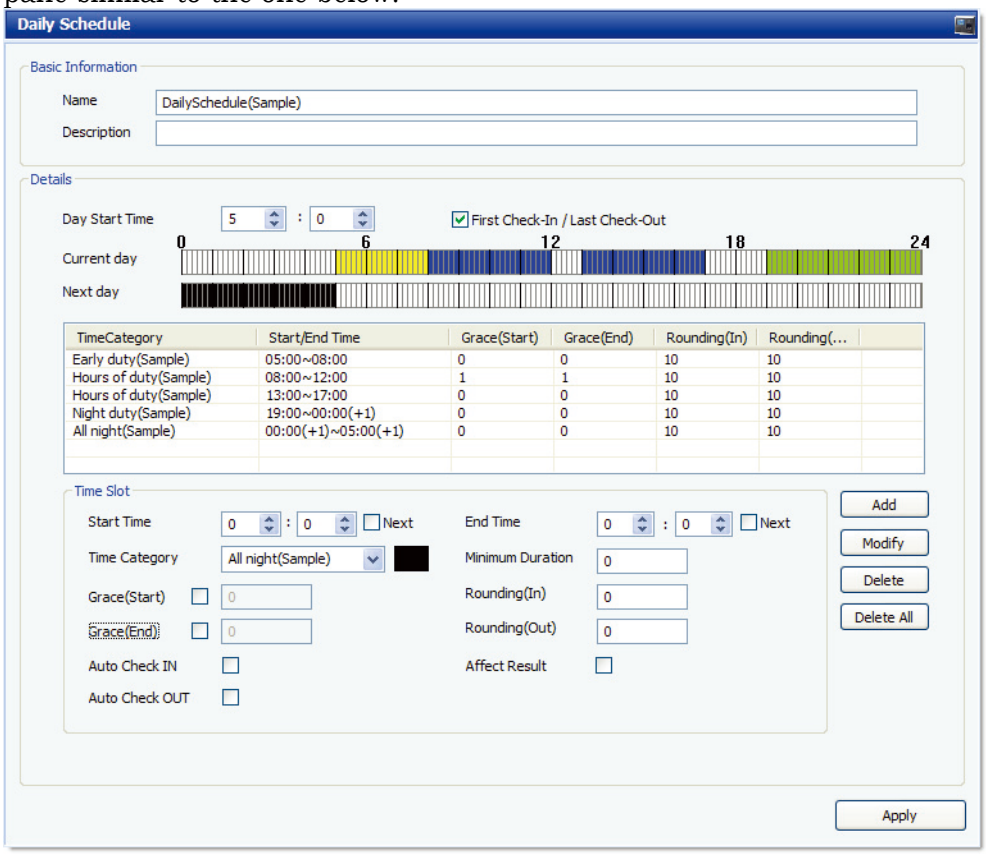


3. Enter a name and description for the time category.
4. Add details for the time category:
   - **Time Rate** - enter the rate at which time is calculated for this time category.
   - **Rounding Unit(Min)** - specify in minutes how to round a user's work time (for example, a entry of "5" will round 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.

3.8.2 Add a Daily Schedule

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:
   a. 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 3.8.1 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.

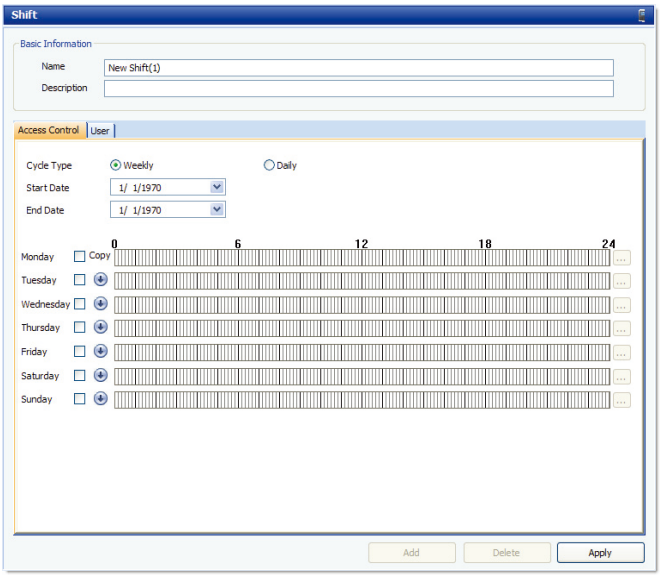
b. Click **Add** to add the time slot to the daily schedule.

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

3.8.3 Add a Shift

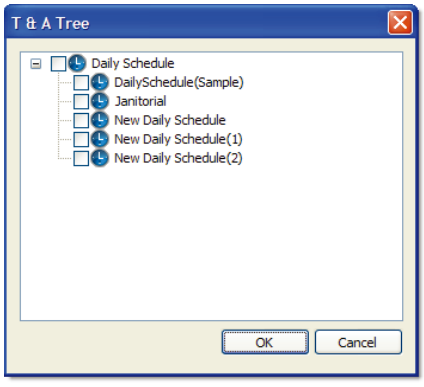
To add a shift,

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 radio 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, 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 window. See section 3.8.2 to define the daily schedules that will appear in this window.



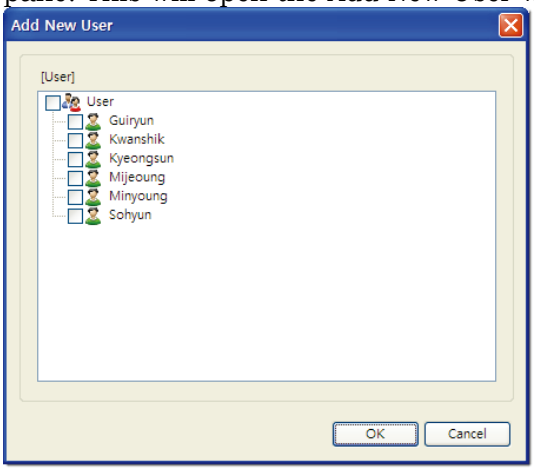
7. Select a daily schedule and click **OK** to apply the daily schedule to the shift.
8. Repeat steps 5-7 as needed.
   Note: You can copy a schedule from one day to the next by clicking the arrow to the right of the day.
9. Click **Apply** to save the shift.

3.8.4 Apply a Shift to Users

You should apply a shift to users so that the BioStar can calculate the users' work time. You can use two methods: applying a shift to users in the Time and Attendance pane or in the User pane.

To apply a shift to users in the Time and Attendance pane,

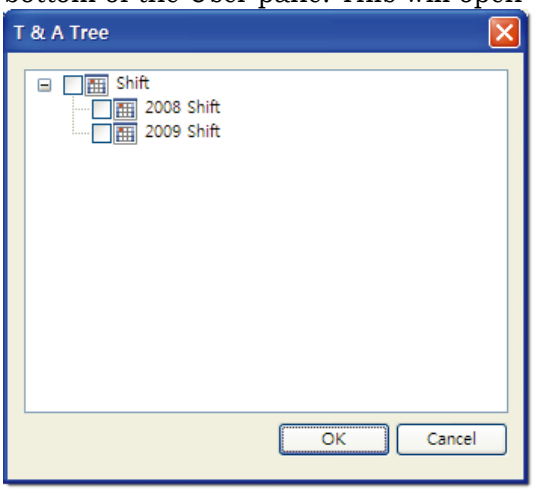
1. Click **Time and Attendance** in the shortcut pane.
2. In the navigation pane, click a shift name.
3. In the Shift pane, click the User tab and then click **Add** at the bottom of the pane. This will open the Add New User window.



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

To apply a shift to users in 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 radio button next to Shift Management and then click **Add** at the bottom of the User pane. This will open the T&A Tree window.

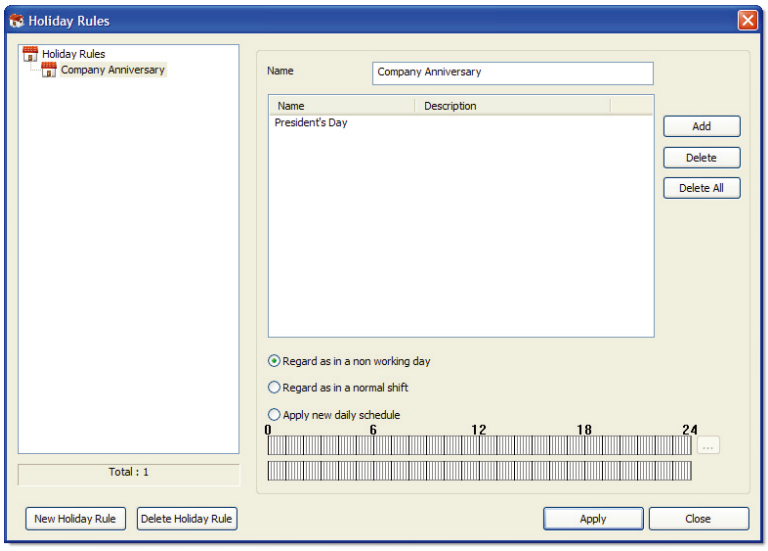


5. Select a shift and click **OK** to apply the shift to the selected user.
6. Click **Apply** to save the T&A settings for the user.

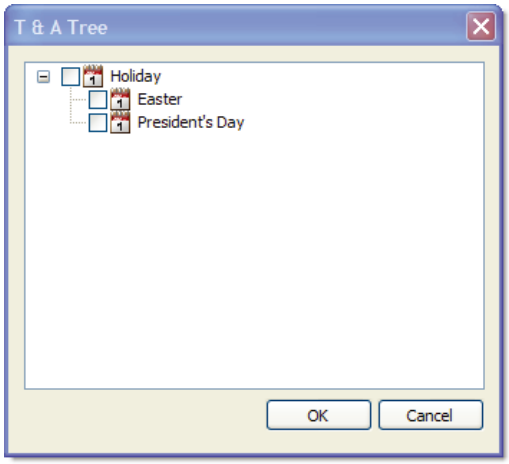
3.8.5 Add a Holiday Rule

To add a holiday rule,

1. Click **Time and Attendance** in the shortcut pane.
2. In the task pane, click *Holiday Management*. This will open the Holiday Rules window.



3. Click New Holiday Rule.
4. Enter a name for the rule.
5. Click **Add**. This will open the T&A Tree window.



6. Select a holiday from the list and click **OK**. To define a holiday, see section 3.6.2.
7. Click one of the radio buttons at the bottom of the Holiday Rules window to specify how the holiday should affect time and attendance schedules:

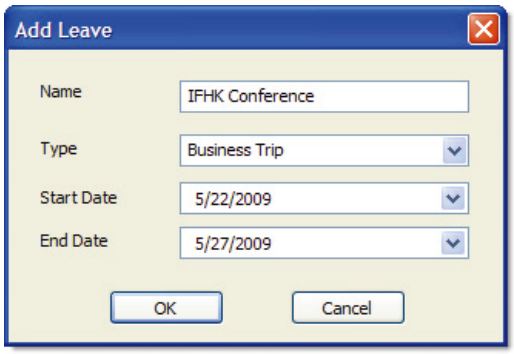
- **Regard as in a non-working day** - time worked on this day is not recorded and does not appear on T&A reports.
- **Regard as in a normal shift** - time worked on this day is recorded and calculated as in a normal shift.
- **Apply a new daily schedule** - time worked on this day is recorded and calculated per a selected daily schedule.

8. If you chose to apply a new daily schedule, click the ellipsis button (...) to select a schedule. See 3.8.2 to create daily schedules.
9. Click **Apply** to save the holiday rule.

3.8.6 Add a Leave Period

Add leave periods to define times when workers are scheduled to be out of the office, but should still be considered to be working, such as paid vacation or business trips. To include a user's scheduled vacation or leave time in the time and attendance settings,

1. Click **User** in the shortcut pane.
2. In the User pane, click the T&A tab.
3. Click the radio button next to Leave Management and then click **Add**. This will open the Add Leave window.



4. Enter a name for the leave period, if desired.
5. Select a leave type from the first drop-down list.
6. Enter the start and end dates for the leave by clicking the drop-down calendars.
7. Click **OK** to add the leave period to the user's T&A settings.
8. Click **Apply** to save the user's T&A settings.

3.9 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).

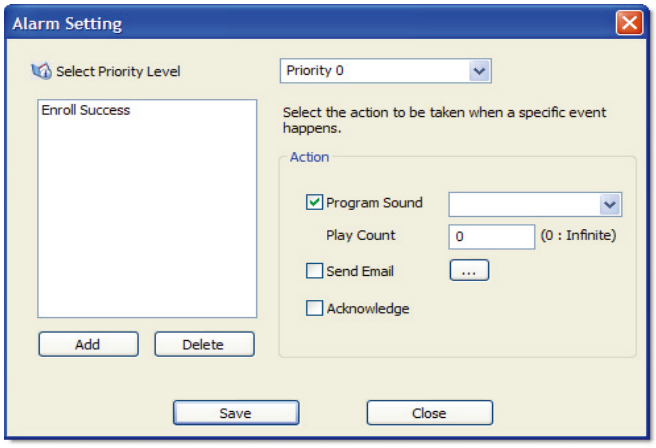
3.9.1 Configure Alarm Settings and Sounds

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.

3.9.1.1 Customize alarm actions

To customize alarm actions,

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



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.
   - If you select *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, see section 3.9.1.2.

- If you select *Send Email*, click the ellipsis button (...) to the right to select an email recipient. To configure email notifications, see section 3.9.2.
- Selecting Acknowledge will activate pop-up alerts on client PCs.

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

3.9.1.2 Add custom alarm sounds

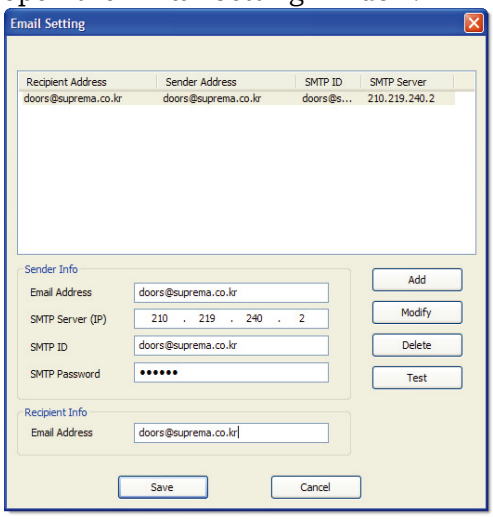
To add custom alarm sounds,

1. From the menu bar, click **Option > Event > Sound Setting**. This will open the Sound Setting window.
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**.

3.9.2 Configure email notifications

BioStar can send email notifications when an alarm event occurs (not available in the free version). As explained in 3.9.1.1, you can customize which events will trigger an automatic email alert. To configure an email notification,

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



2. Type the email address, SMTP server, SMTP ID, and SMTP password in the *Sender Info* section.
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**.

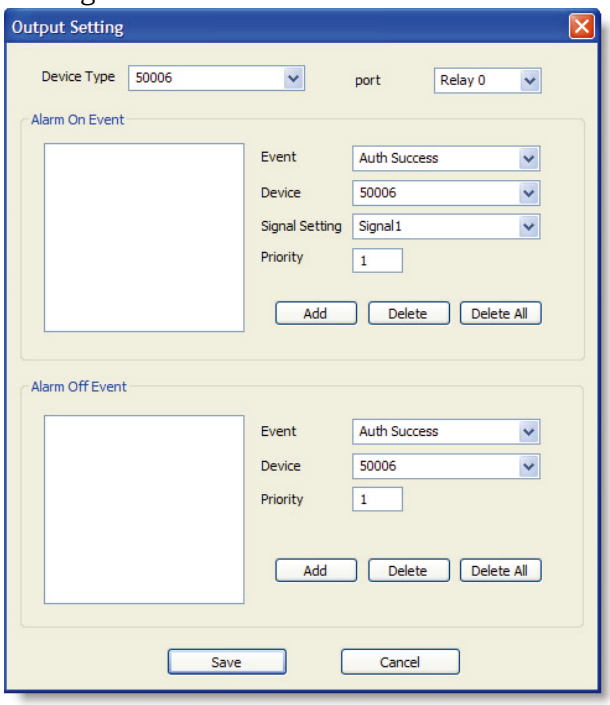
3.9.3 Configure Settings for External Devices

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.

3.9.3.1 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 window.

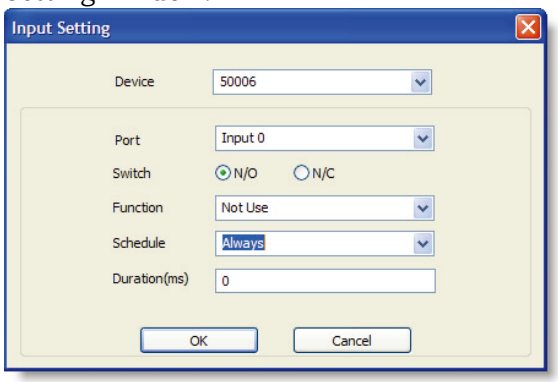


5. Configure actions that will activate (send a signal to) a specified output relay:
   a. In the *Alarm On Event* section, select an event from the first drop-down list.
   b. Select the device number or *All Device* from the second drop-down list.
   c. Select a signal setting from the third drop-down 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**.

3.9.3.2 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 window.



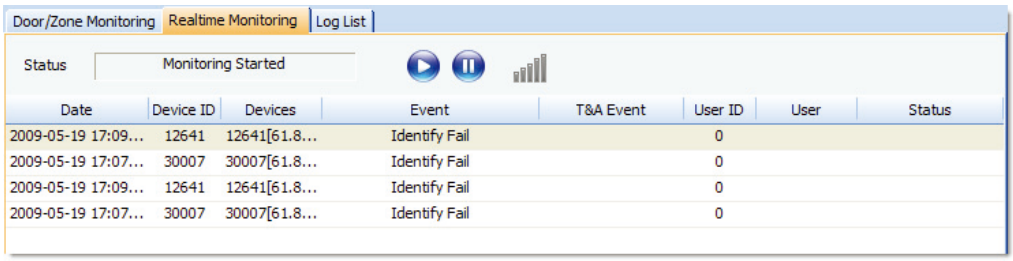
5. Select an input port from the second drop-down list.
6. Select the normal position of the input switch (*N/O-normally open* or *N/C-normally closed*).
7. Select a function for the input (*Not Use*, *Generic Input*, *Emergency Open*, *Release All Alarms*, *Restart Device*, or *Disable Device*).
8. Select a schedule for applying the function (*Always*, *Disable*, or custom schedules).
9. Set the minimum duration (in milliseconds) an input signal must last to trigger the specified action.
10. Click **OK**.

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, 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.

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. You can also use the Log List tab in the Monitoring pane to specify log parameters.

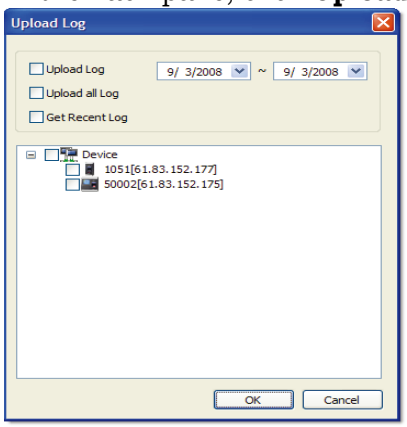
BioStar automatically collects log information from connected devices as long as the server is running. However, if you have devices that are not connected to the BioStar server, you must manually upload logs before viewing them.

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 window.

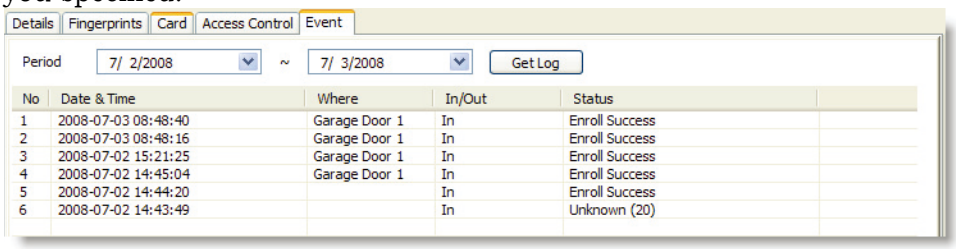


4. Select an upload option by clicking the corresponding box:
   a. **Upload Log** - Use this option to upload logs for a specific time period. Specify the period with the drop-down calendars.
   b. **Upload All Log** - Use this option to upload all logs.
   c. **Get Recent Log** - Use this option to upload logs written since the previous upload.
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.

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.

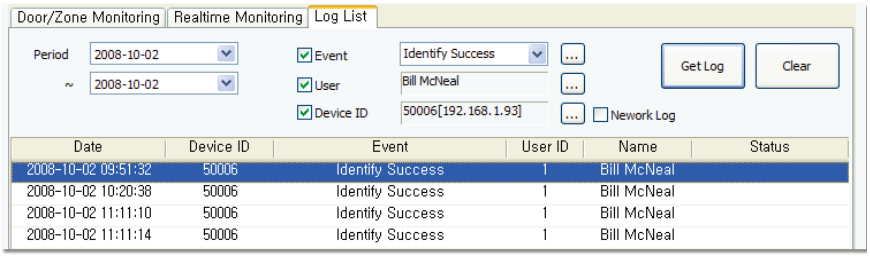


4.2.3 View Logs from the Monitoring Pane

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 window.
   - To show events by user, click the User checkbox and then click the ellipsis button (...) to select a user or users from the User/Department Tree window. 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 window. 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.

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



4.3 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.

4.3.1 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**.

4.3.2 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**.

4.3.3 Lock or Unlock Devices

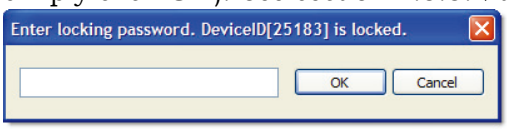
BioStar allows you to lock and unlock devices to prevent unauthorized access when BioStar is not running. This action blocks communication from devices. You can either lock devices manually from the BioStar interface or automatically when you exit the BioStar software. All connected devices can be simultaneously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

4.3.3.1 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,

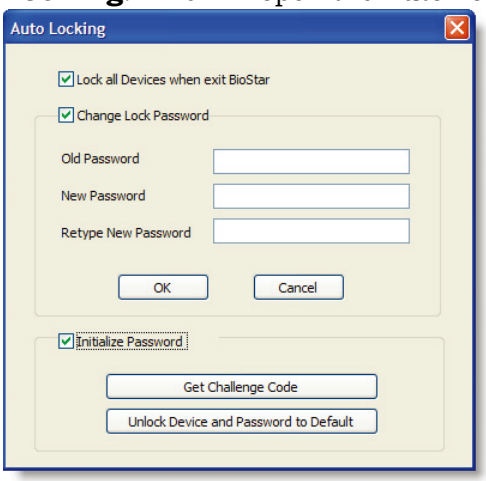
1. From the menu bar, click **Option > Device > Unlock All Devices**.
2. If necessary, enter a password in the Enter Locking Password window and click **OK** (if you have not created a locking password, simply click **OK**). See section 4.3.3.2 to create a locking password.



4.3.3.2 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 window.

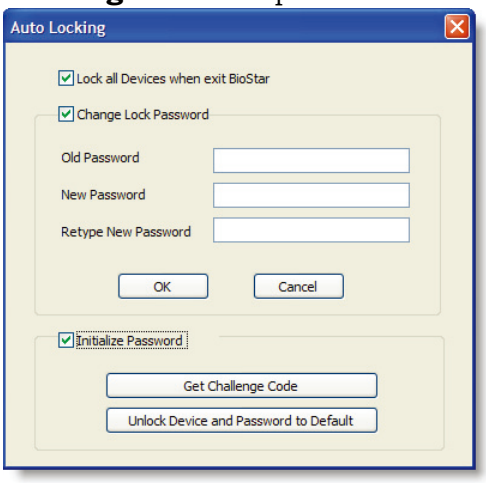


2. Click the first checkbox to lock all devices when exiting BioStar.
3. If desired, click the second checkbox to change the lock password:
   a. Enter the old password
   b. Enter the new password
   c. Retype the new password to confirm.

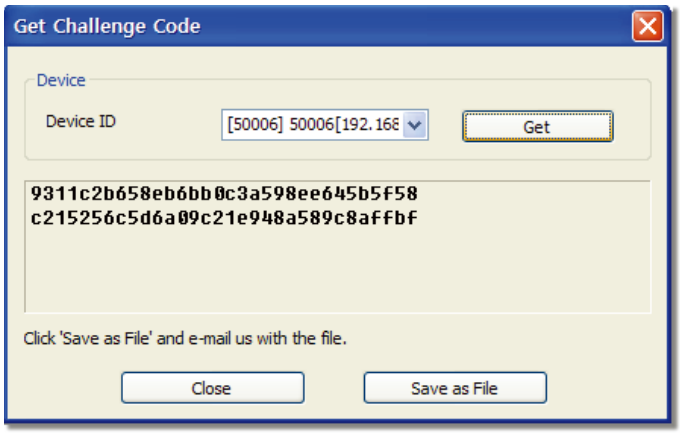
4.3.3.3 Reset a device lock

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 window.

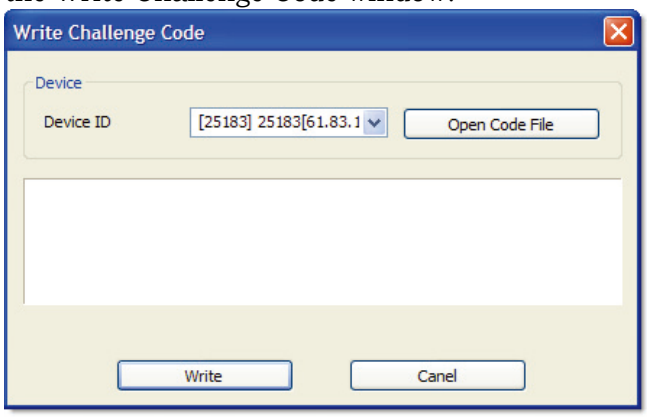


2. Click the Initialize Password checkbox to activate the buttons at the bottom of the window.
3. Click Get Challenge Code. This will open the Get Challenge Code window.



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 window and activate the buttons (see steps 1-3).
8. Click **Unlock Device and Password to Default**. This will open the Write Challenge Code window.



9. Click **Open Code File** and locate the file sent to you by Suprema.
10. When you have opened the file, click **Write**. This will unlock the device and reset the locking password to the default (no password).

4.4 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.

4.4.1 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.

4.4.1.1 Delete users via command cards

After issuing command cards, you can delete a user (or all users) directly from a BioEntry Plus device. For more information about issuing command cards, see section 3.2.5.1. To delete users via command cards,

1. Place a delete (or delete all) card on a BioEntry Plus device.
2. If authorization is required, an administrator must scan his or her fingerprints to continue.
3. When deleting a single user, place the user's access card on the device or have a user place his or her finger on the scanner (as prompted by the device).
4. When deleting all users, place the delete card on the BioEntry Plus device again to confirm the action.

4.4.2 Transfer Users to Other Departments

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

1. Click **User** in the shortcut pane.
2. In the navigation pane, right-click *User*.
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.

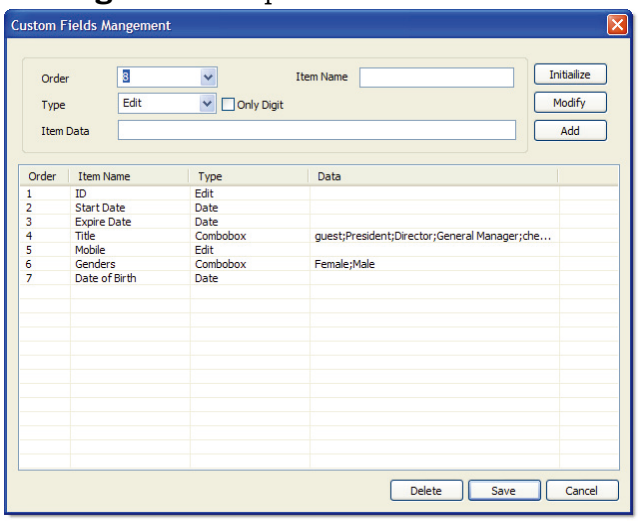
4.4.3 Customize User Information Fields

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

4.4.3.1 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 window.



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**.

4.4.3.2 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 window (see section 4.4.3.1).
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 window.

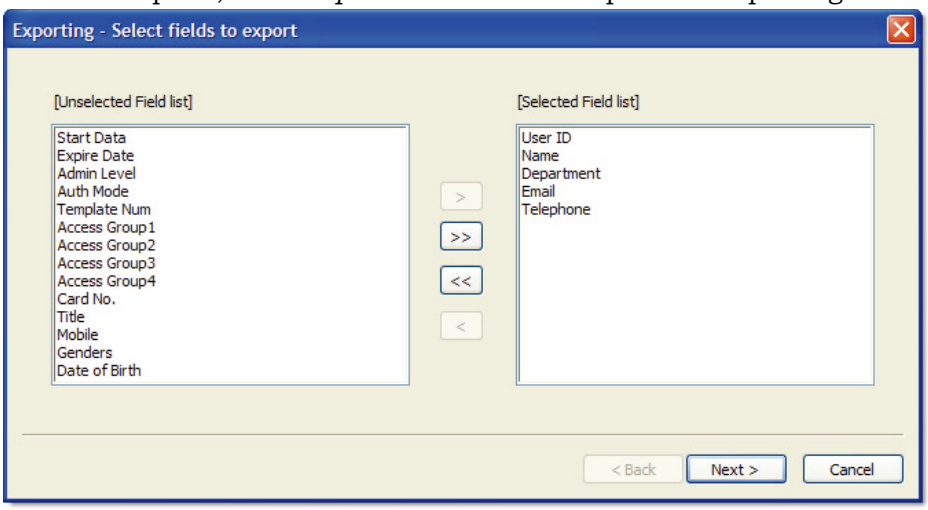
Note: Items 1-4 are required fields and cannot be modified or deleted.

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**.

4.4.4 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 window.

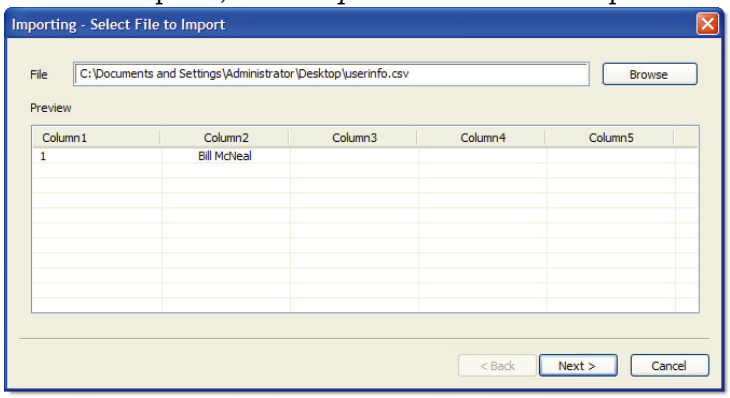


3. Select types of user data to export by clicking items in the list on the left and then clicking **>**.
4. After selecting all the types of user data to export, click **Next**.
5. Type a path and filename for the user data or click **Browse** to select a location to save the file.
6. Click **Next**.
7. Click **Export** to begin exporting the user data.
8. When the export is complete, click **Finish**.

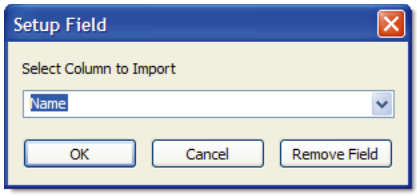
4.4.5 Import User Data

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 window.



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 window, 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**.
7. Repeat steps 5-6 as necessary to map additional data.
8. When you are finished mapping data to fields, click **Next**.
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**.

4.5 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.

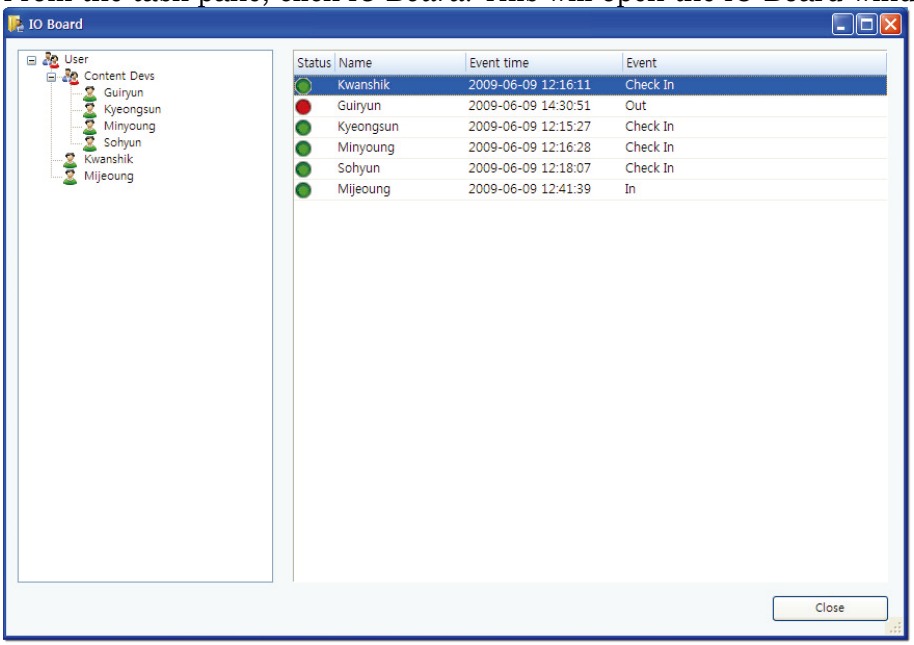
4.5.1 Monitor T&A Status via the IO Board

The IO Board displays time and attendance events. The IO Board does not track every come-in and go-out event done by users, but does track only the come-in and go-out events done by users using the T&A function keys of the access control devices.

Note: The IO Board is available only with 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 window.

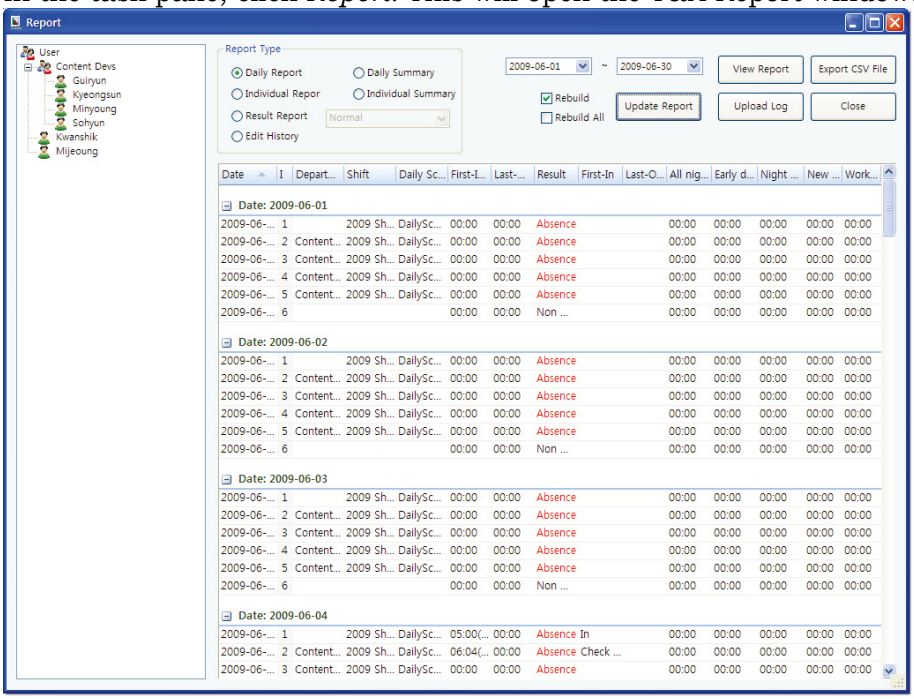


3. Click **User**, a user name, or a department name in the pane on the left. This will display the corresponding T&A status in the pane on the right.
4. To close the window, click **Close**.

4.5.2 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 window.

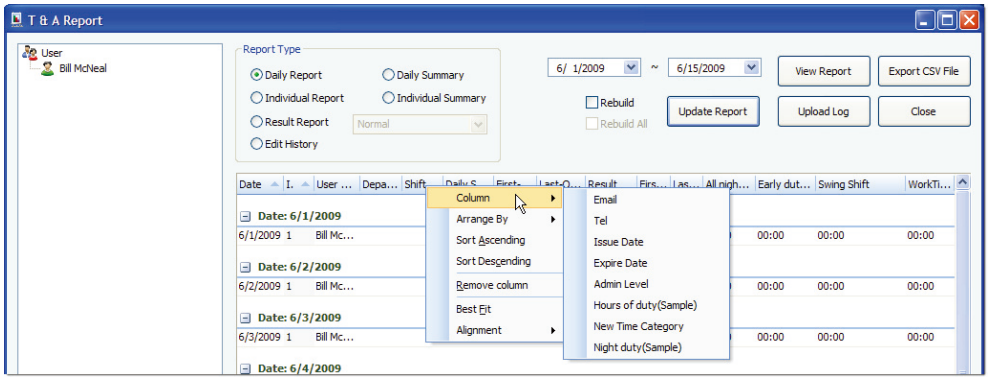


3. Click a radio button to select a report type:
   - **Daily Report** - a report of all activities for the specified date range sorted by date.
   - **Individual Report** - a report of activities for the specified date range sorted by user ID.
   - **Result Report** - a report of activities that you 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.
4. Select a date range by clicking the drop-down calendars.
5. Click **View Report** to retrieve and display the results.

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.

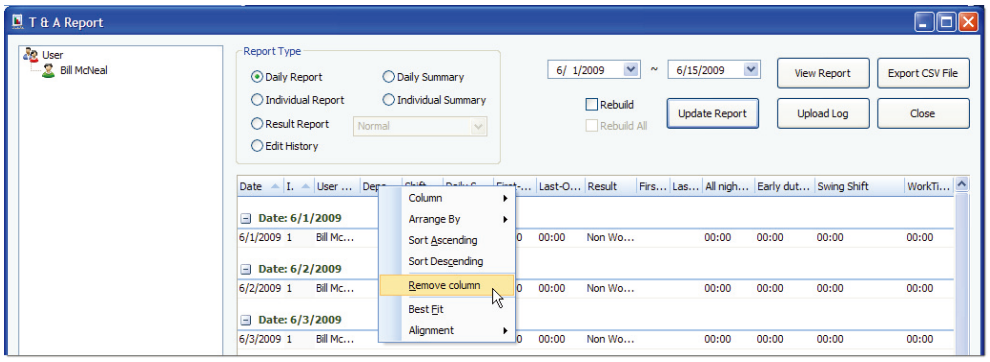
To add a column to the report,

1. Right-click on any column header.
2. Point to **Column** and select a column in the list.



To remove a column from the report,

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



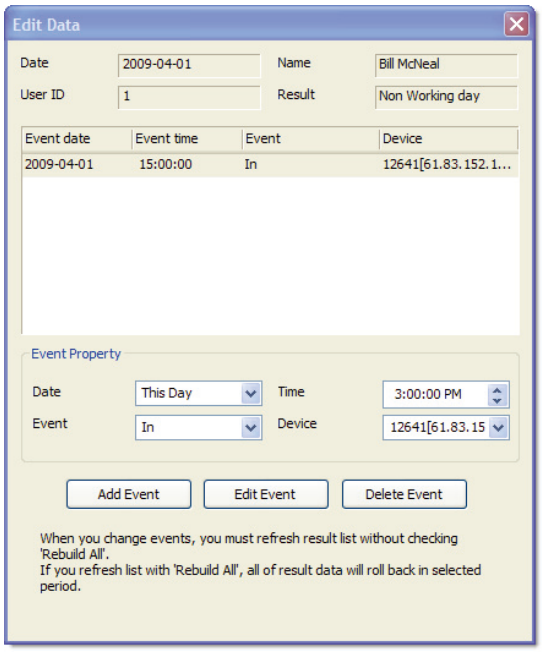
Note: Clicking **Upload Log** will retrieve data from all networked devices, while **Update Report** will refresh the report with any data you have modified (see section 4.5.3).

4.5.3 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 window.



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 window.

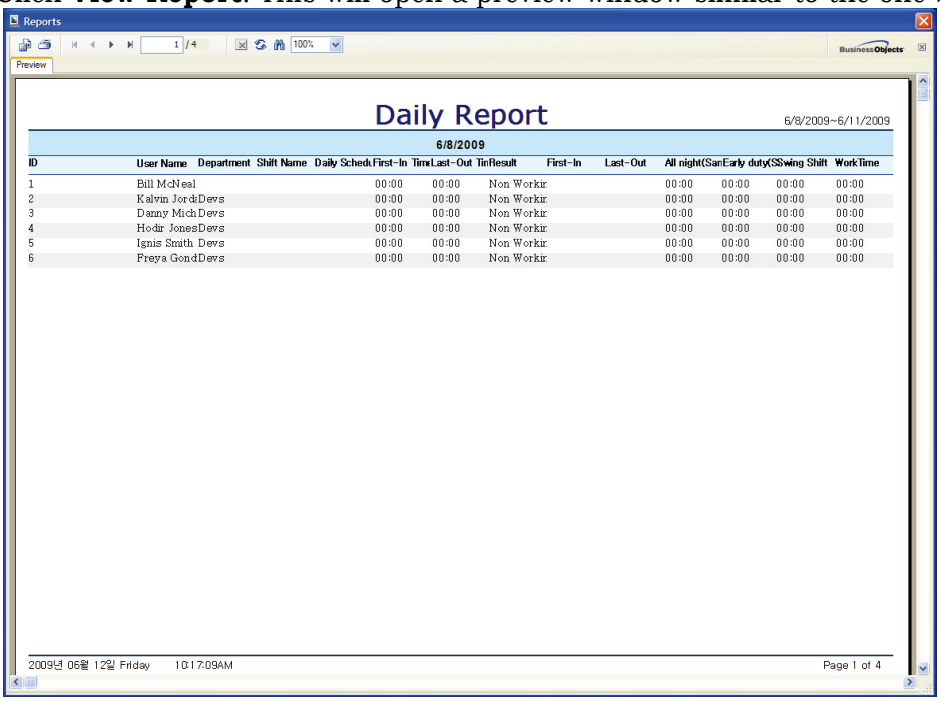
5. In the T&A Report window, ensure that the “Rebuild” checkbox is NOT checked.
6. Click **Update Report**. The report will show the changes you have made. The changes you have made via the detailed editing will not be restored to the original data even if you click the check box next to “Rebuild” and 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.

4.5.4 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.
2. If necessary, make modifications as described in 4.5.3.
3. Click **View Report**. This will open a preview window similar to the one below.



4. To print the report, click the print icon on the toolbar.
5. To export the report data, click the export icon on the toolbar and then select an export format and a destination. You can export the data in the following formats:
   - Adobe Acrobat (PDF)
   - Crystal Report (RPT)

- HTML 3.2
- HTML 4.0
- Microsoft Excel 97-2000 (XLS)
- Microsoft Excel 97-2000 – Data only (XLS)
- Microsoft Word (RTF)
- Microsoft Word – Editable (RTF)
- ODBC
- Record Style – Columns with spaces (REC)
- Record Style – Columns with spaces (REC)
- Report Definition (TXT)
- Rich Text Format (RTF)
- 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.

4.6 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.

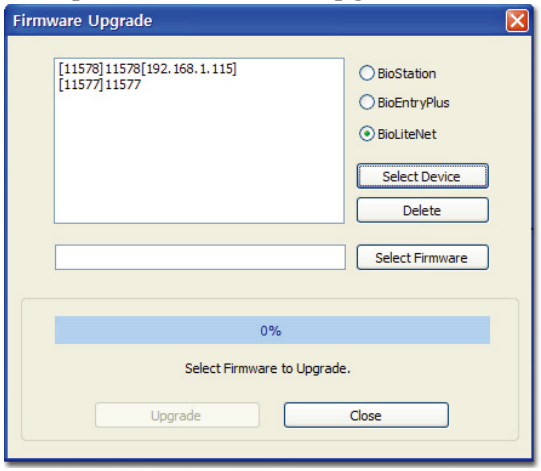
4.6.1 Remove Devices

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*.

4.6.2 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 window.



2. Click the radio 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 window.
4. Click **OK** to close the Device Tree window.
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 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 window.
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 window.
   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.

4.8 Change the Fingerprint Template

BioStar offers two types of fingerprint templates: the ISO 19794-2 format 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. To change the fingerprint template option,

1. From the menu bar, click **Option > Fingerprint**. This will open the Fingerprint window.
2. Click the checkbox under “Template Format Option” to select the ISO 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

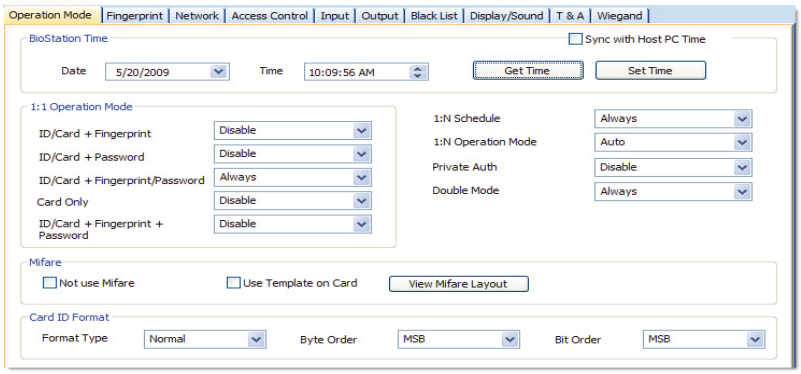
While most device settings are similar for BioStation, BioEntry Plus, and BioLite Net devices, the devices provide slightly different capabilities. The sections that follow describe the settings for each device separately. To access the tabs described below, click **Device** in the shortcut pane, then 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.

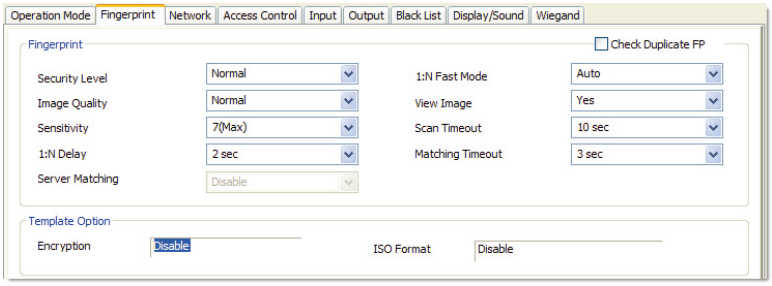


- **BioStation Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set 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, see section 3.5.3.6.
- **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 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*) least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) 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.

5.1.1.2 Fingerprint tab

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



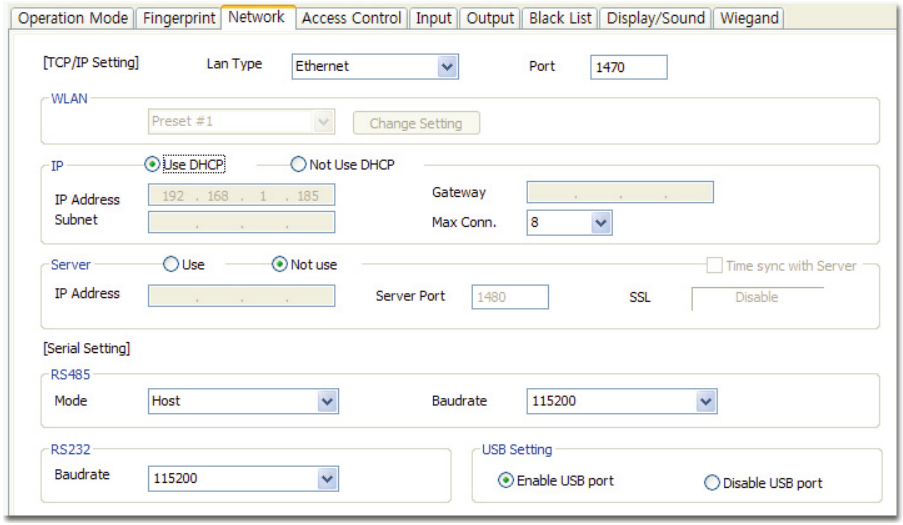
- **Fingerprint**
  - **Security Level** - set the security level to use for fingerprint authorization (*Normal*, *Secure*, or *Most Secure*). Keep in mind that as the security level is increased, so too is the likelihood of a false rejection.
  - **Image Quality** - set the strictness of the quality 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 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, see section 3.2.4.1.
- **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
- **Not Use DHCP** - click this radio 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 radio button to enable the server mode.
- **Not use** - click this radio 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.
- **SSL** - displays the status of SSL for the server connection.
- **Time sync with Server** - check this box to synchronize the device time with the time maintained at the server.

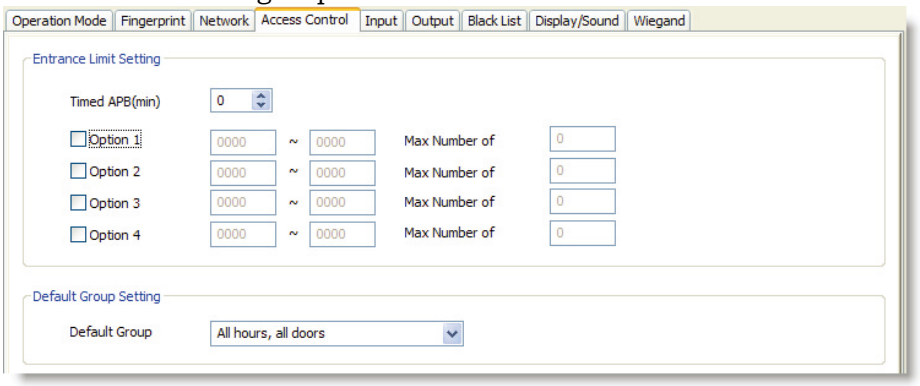
• **RS485**
- **Mode** - set the mode for a device connected via RS485 (*Disable*, *Host*, *Slave*, or *PC Connection*). For more information about RS485 modes, see sections 3.2.1 and 3.2.2.
- **Baudrate** - set the baud rate for a device connected via RS485 (*9600* to *115200*).

• **RS232** - set the baud rate for a device connected via RS232 (9600 to 115200).

• **USB Setting** - click the radio buttons to enable or disable the USB port on the BioStation device.

5.1.1.4 Access Control tab

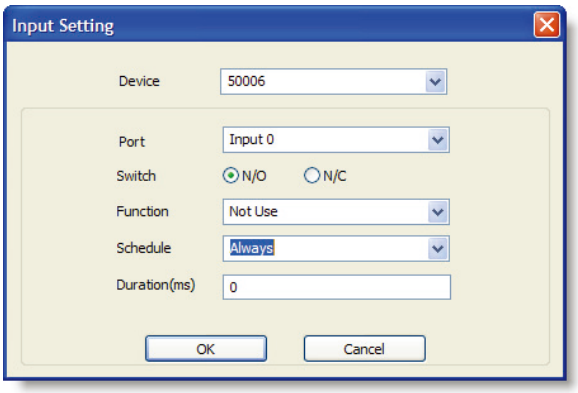
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioStation device.



- **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 window. For more information about configuring input settings, see section 3.9.3.2.



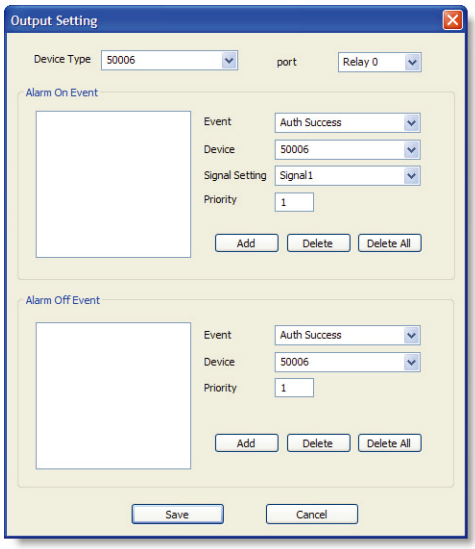
- **Device** - select the BioStation (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to specify 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 settings window—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 4.3.1).
  - **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 device.

- **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 window. For more information about configuring output settings, see section 3.9.3.1.



- **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.

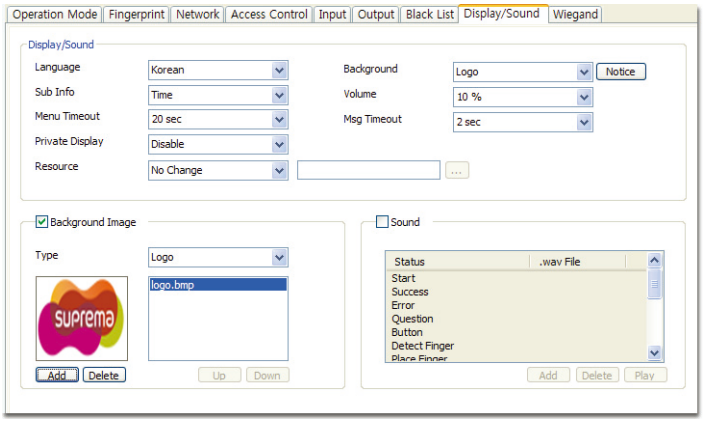
- **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, 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 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

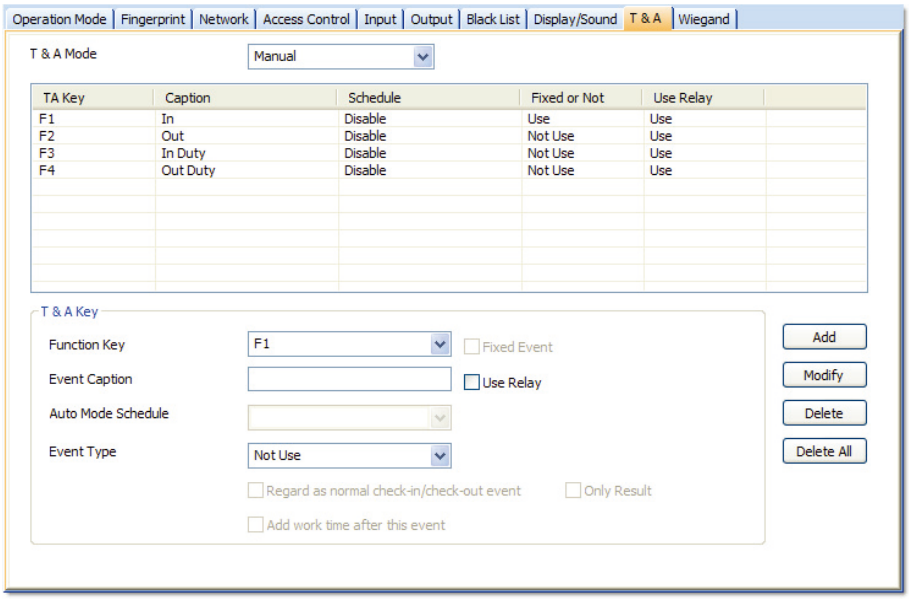
one image at a time can be used as a logo or notice, while up to 16 images can be displayed (at a set interval) in a slide show.

- **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.

5.1.1.8 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**.



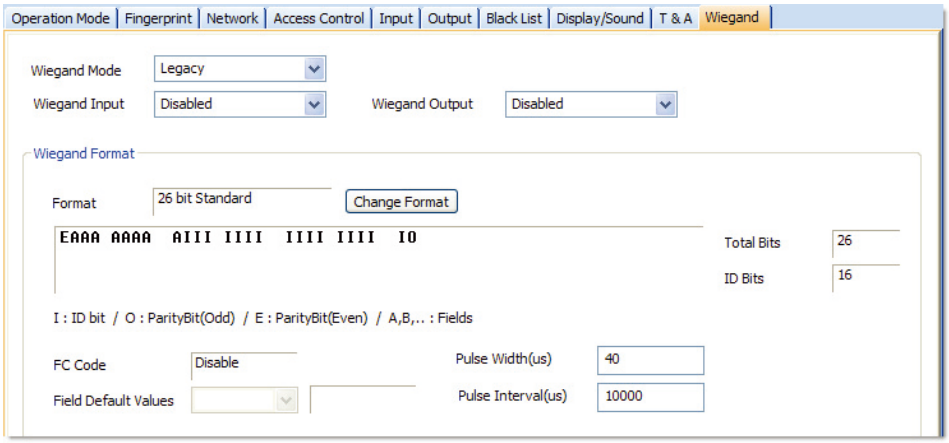
- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.

  - **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, see section 3.6.1.
  - **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.

5.1.1.9 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 3.2.7.



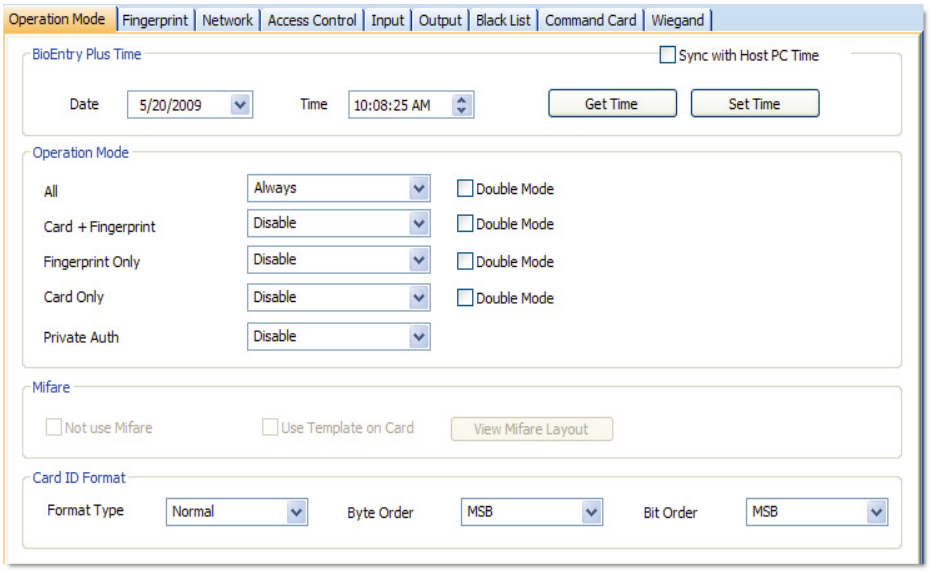
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate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

The sections below describe the settings available for BioEntry Plus devices. Customize the way BioEntry Plus 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 devices.



- **BioEntry Plus Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set 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**

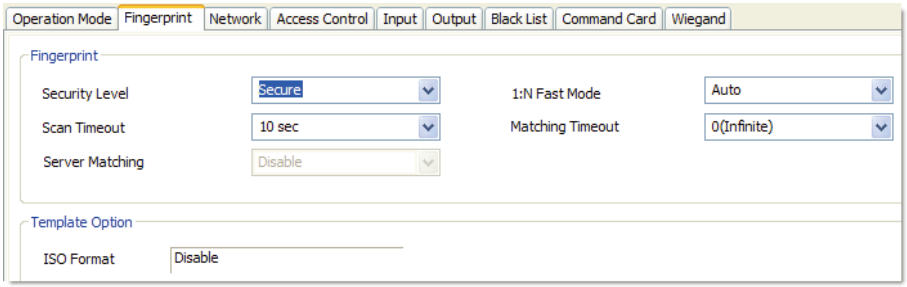
- **Not use Mifare** - check this box to disable MIFARE card authorization.
- **Use Template on Card** - check this box to use the template on the MIFARE card for authorization.
- **View Mifare Layout** - click this button to configure the MIFARE layout used by the device. For more information about configuring MIFARE layouts, see section 3.5.3.6.

• **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 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*) least significant byte (*LSB*).
- **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) least significant bit (*LSB*).

5.1.2.2 Fingerprint tab

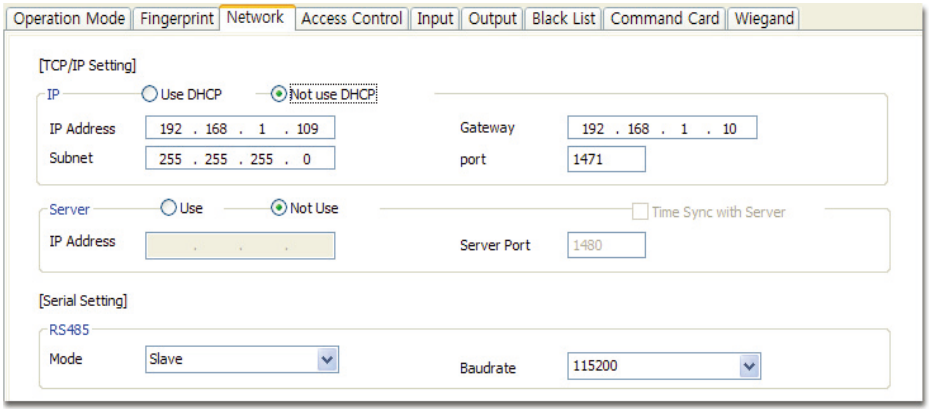
The Fingerprint tab allows you to customize fingerprint authorization settings for BioEntry Plus devices.



- **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.
  - **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*).

5.1.2.3 Network tab

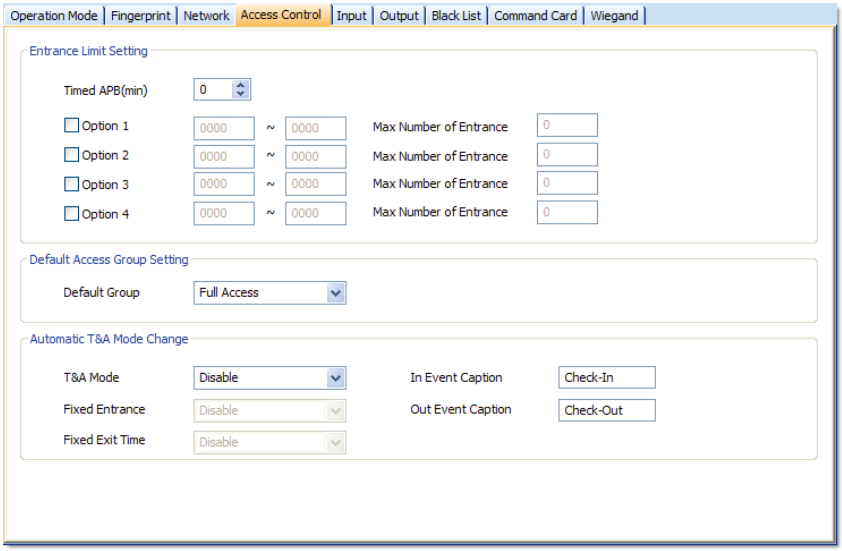
The Network tab allows you to customize network and server settings for BioEntry Plus devices.



- **TCP/IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio 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 radio button to use specific server settings.
  - **Not use** - click this radio 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 time maintained at the server.
- **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*).

5.1.2.4 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 device.



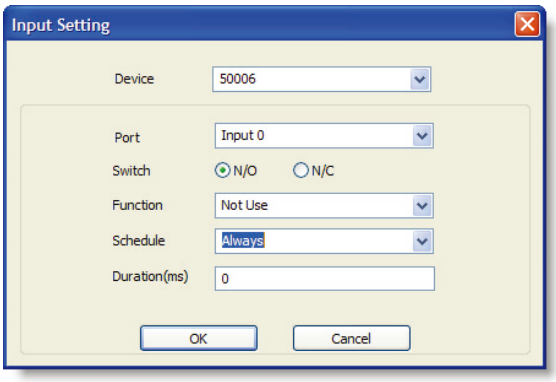
- **Entrance Limit Setting**
  - **Timed APB (min)** - set the duration (in minutes) that a user will be unable to regain entry to an area via the device. Once a user has gained entry, the device will reject the user's card or fingerprint authorization for the time period specified here.
  - **Option 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, see section 3.6.1.
  - **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, see section 3.6.1.

- **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 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 window. For more information about configuring input settings, see section 3.9.3.2.



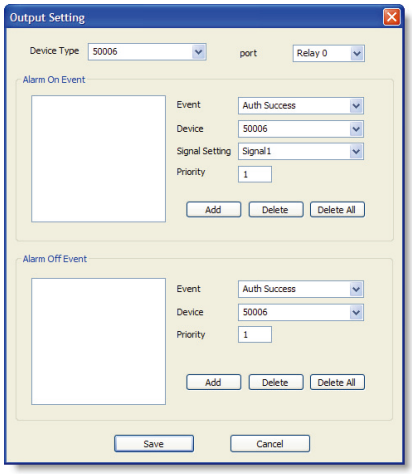
- **Device** - select the BioEntry Plus (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (Input 0, Input 1, or Tamper). For Secure I/O devices, these settings are available: Input 0, Input 1, Input 2, Input 3.
- **Switch** - click the radio buttons to 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 settings window—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 4.3.1).
  - **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 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.

5.1.2.6 Output tab

The Output tab lists output settings you have specified for a BioEntry Plus 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 window. For more information about configuring output settings, see section 3.9.3.1.



- **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*).

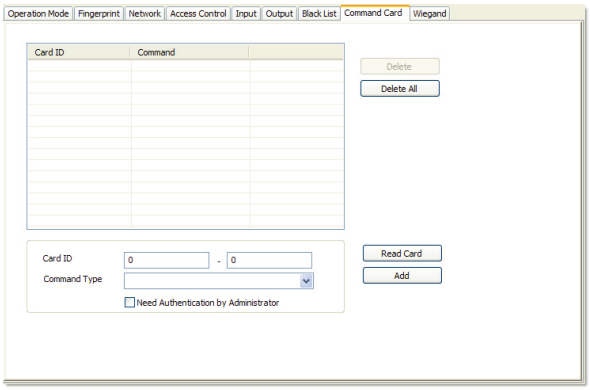
- **Device** - select the device to monitor for an alarm event.
- **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (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 Command Card tab

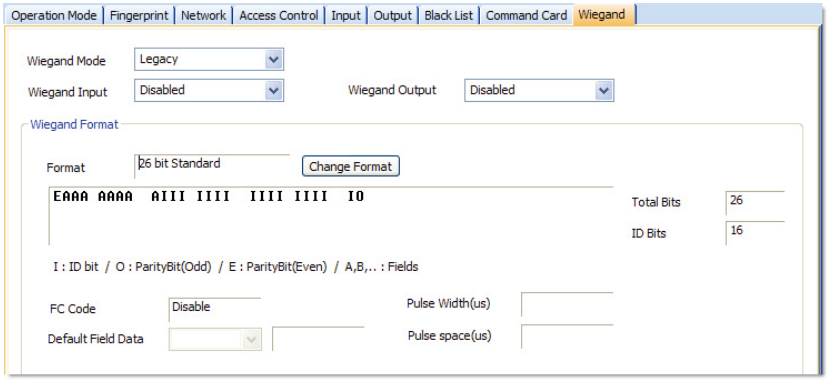
The Command Card tab allows you to issue command cards. For more information about command cards, see section 3.2.5.1.



- **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*).

5.1.2.8 Wiegand tab

The Wiegand tab allows you to configure the Wiegand format for a BioEntry Plus device. Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for a BioEntry Plus device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.7.



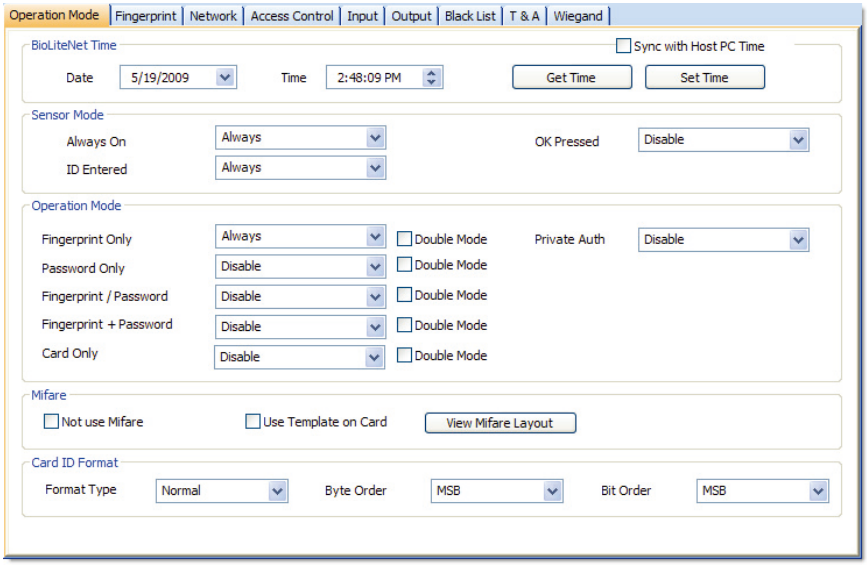
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or *Extended*). The Legacy mode will treat connected RF devices as part of their host devices (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card readers to operate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

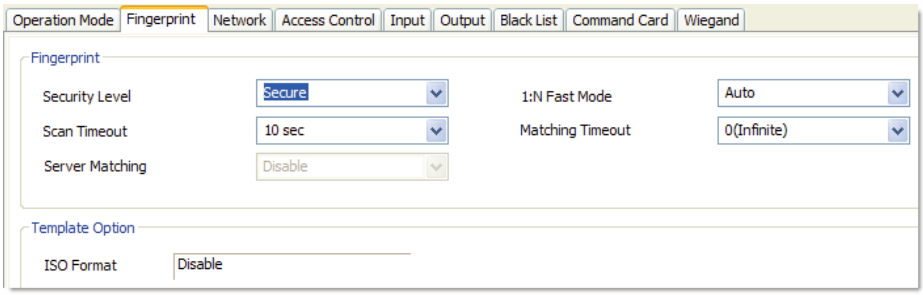


- **BioLiteNet Time**
  - **Date** - manually set the device date with a drop-down calendar.
  - **Time** - manually set the device time.
  - **Sync with Host PC Time** - check this box to automatically synchronize the device time with the time of the host computer.
  - **Get Time** - get the current time displayed by the device.
  - **Set 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, see section 3.5.3.6.
- **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 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*) least significant byte (*LSB*).
  - **Bit Order** - specify whether to swap ID card data between cards and devices by most significant bit (*MSB*) least significant bit (*LSB*).

5.1.3.2 Fingerprint tab

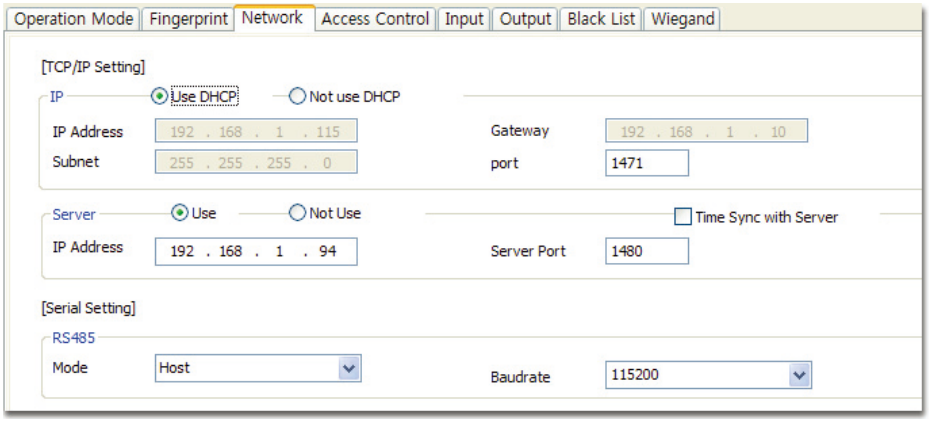
The Fingerprint tab allows you to customize fingerprint authorization settings for BioLite Net devices.



- **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.
  - **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*).

5.1.3.3 Network tab

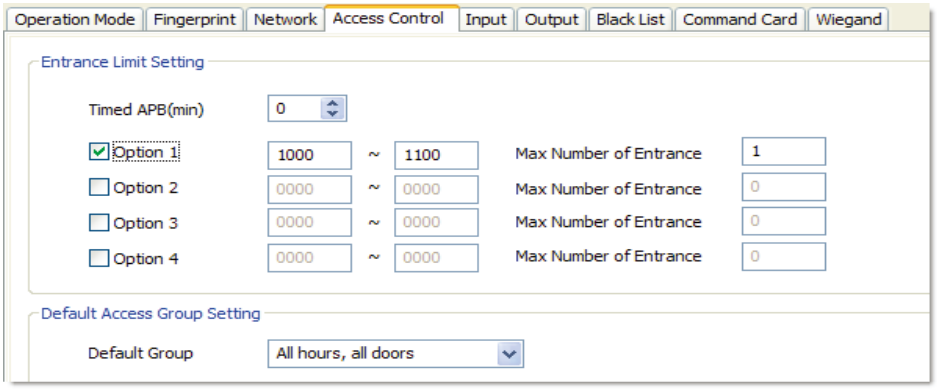
The Network tab allows you to customize network and server settings for BioLite Net devices.



- **TCP/IP**
  - **Use DHCP** - click this radio button to enable the dynamic host configuration protocol (DHCP) for the device.
  - **Not Use DHCP** - click this radio 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 radio button to use specific server settings.
  - **Not use** - click this radio 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 time maintained at the server.
- **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

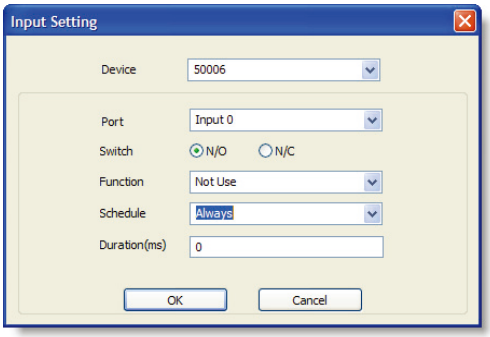
The Access Control tab allows you to customize entrance limit settings and default access groups for a BioLite Net device.



- **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 window. For more information about configuring input settings, see section 3.9.3.2.

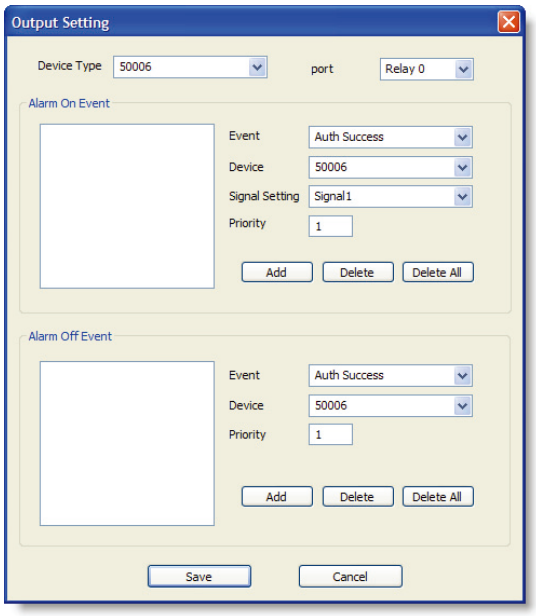


- **Device** - select the BioLite Net (or Secure I/O) device for which you will add or modify settings.
- **Port** - select an input port (*Input 0*, *Input 1*, or *Tamper*). For Secure I/O devices, these settings are available: *Input 0*, *Input 1*, *Input 2*, *Input 3*.
- **Switch** - click the radio 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 settings window—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 4.3.1).
  - *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.

- **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 window. For more information about configuring output settings, see section 3.9.3.1.



- **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.

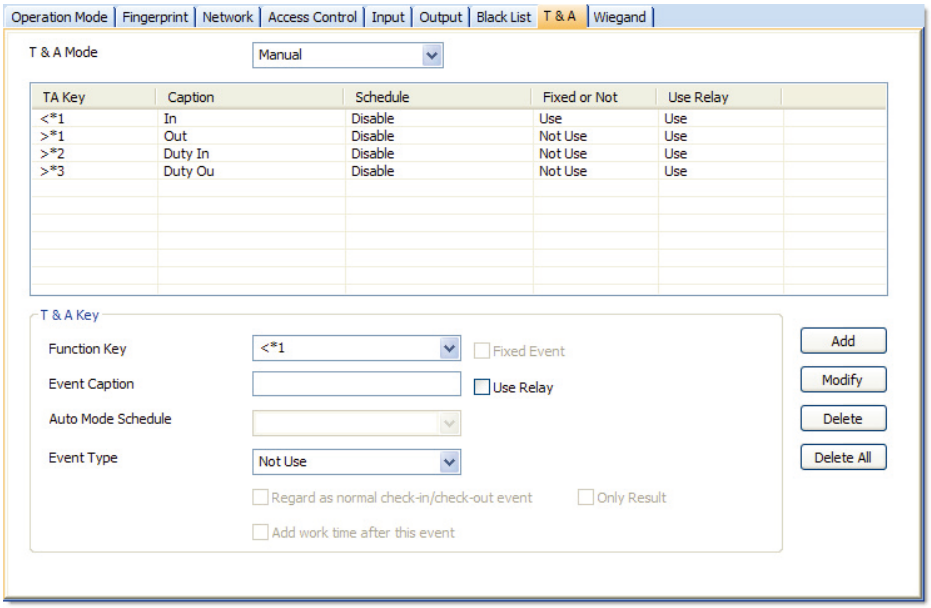
- **Signal Setting** - select a signal setting that you have previously configured from the menu bar (**Option > Event > Output Port Setting**).
- **Priority** - set a priority for the event. Only an event with an equal or higher priority (1 is the highest) can override a previous event. For example, 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 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**.

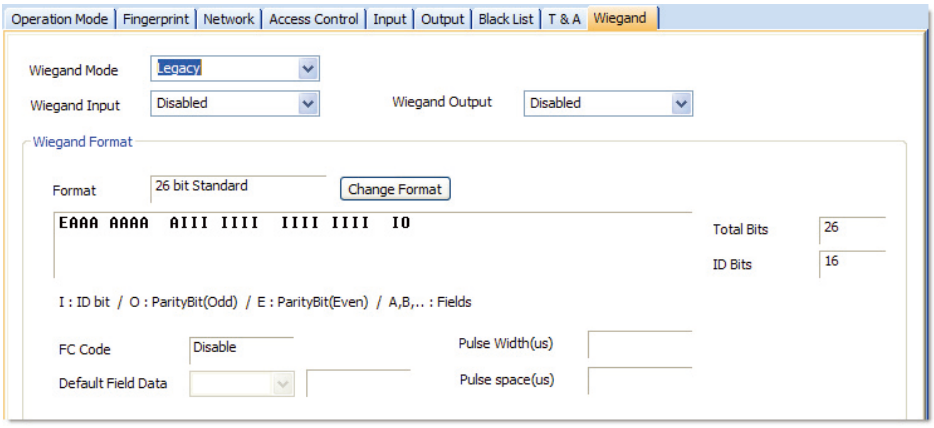


- **T&A Mode** - set the time and attendance mode:
  - **Not Use** - disable the time and attendance functions for this device.
  - **Manual** - users must press the specified key every time they enter or leave to record their T&A events.
  - **Manual Fix** - when a T&A key is pressed, the device will 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, see section 3.6.1.
- **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.

5.1.3.8 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). Click **Change Format** to launch the Wiegand Configuration wizard. To activate the Wiegand feature for a BioLite Net device, click the checkbox at the top right of the tab. For more information on configuring the Wiegand format, see section 3.2.7.



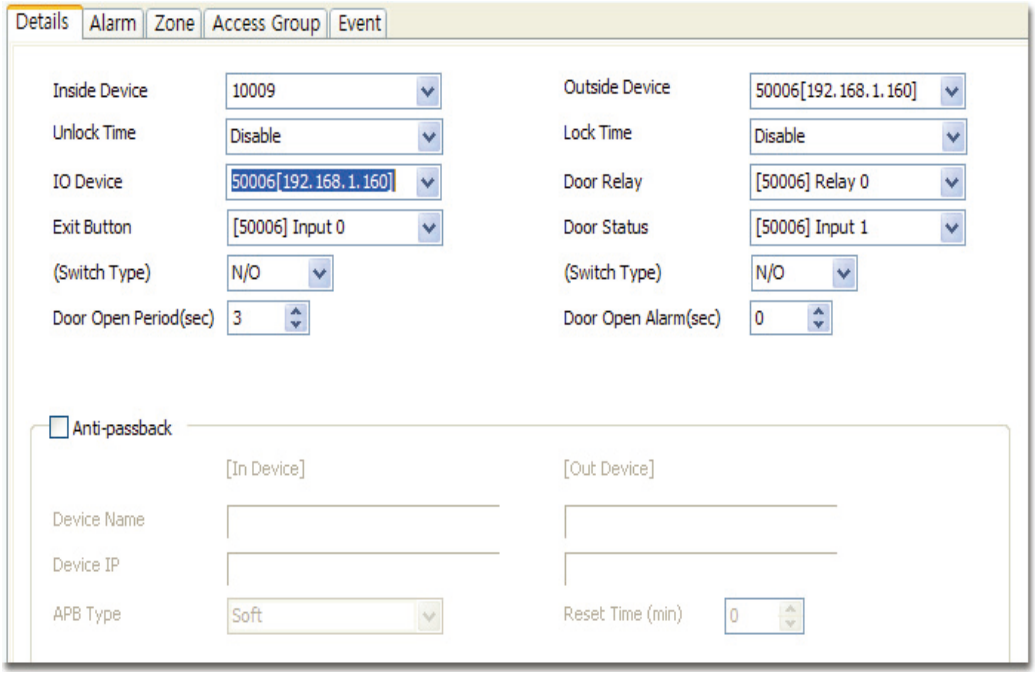
- **Wiegand Mode** - set the mode of Wiegand input to use when reading card ID data (*Legacy* or Extended). The Legacy mode will process ID data from networked devices and RF card readers in the same way (this is the typical function of previous versions of BioStar). The Extended mode will allow RF card 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.

5.2 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.

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.

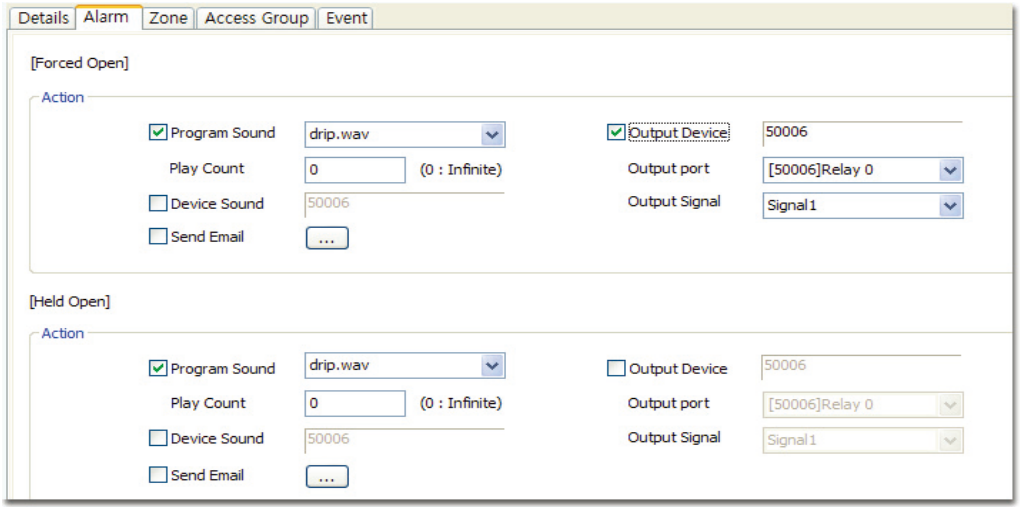


- **Inside Device** - select a device to use on the inside of the door.
- **Outside Device** - select a device to use on the outside of the door.
- **Unlock Time** - select a schedule when the door should normally be unlocked. During this time, door relays are active.
- **Lock Time** - select a schedule 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.
- **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.

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 3.9.1.2.
  - **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 3.9.2.
  - **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 Customize Zone Settings

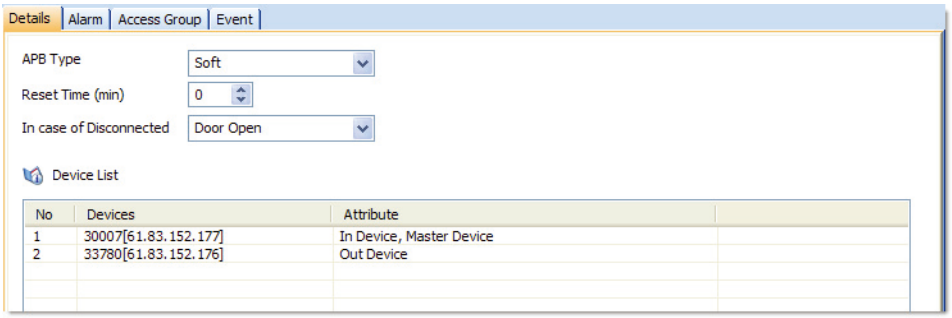
Customize the way zones function by changing the settings to suit your particular environment and operational needs. To access the tabs described below, click **Doors** in the shortcut pane, then click a zone name.

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.

5.3.1.1 Details tab

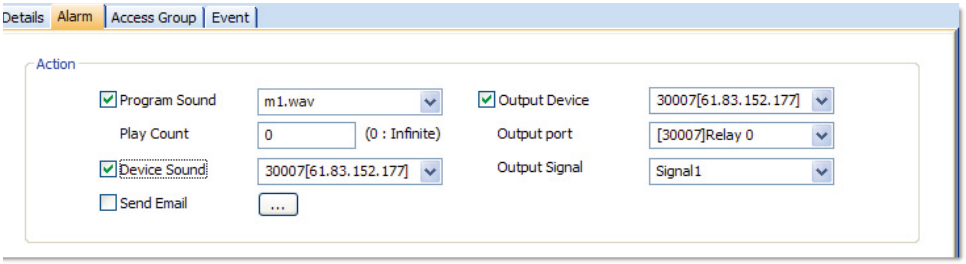
The Details tab allows you to specify which anti-passback type to use for a zone and the reset period for the anti-passback feature.



- **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

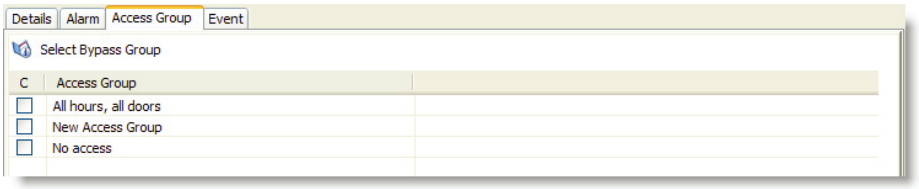
The Alarm tab allows you to specify alarm actions and an output device for an anti-passback zone.



- **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 3.9.1.2.
  - **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 3.9.2.
  - **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 **Add** at the bottom right of the Zone pane.

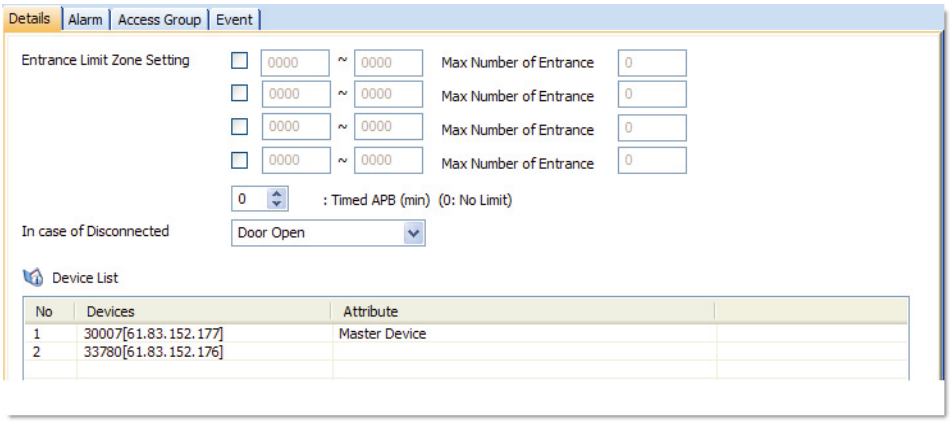


5.3.2 Customize Settings for Entrance Limit Zones

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

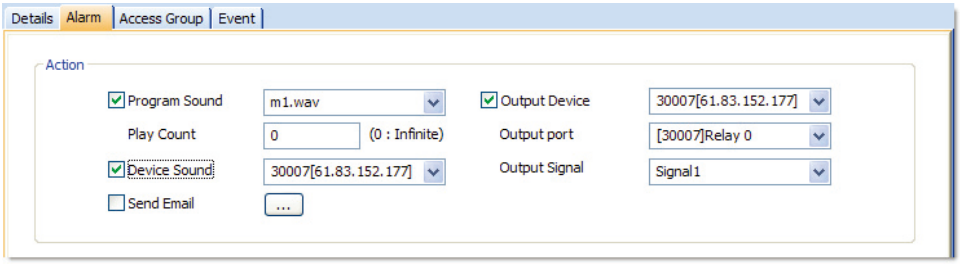
The Details tab allows you to specify entrance limits and a schedule for the zone restrictions.



- **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

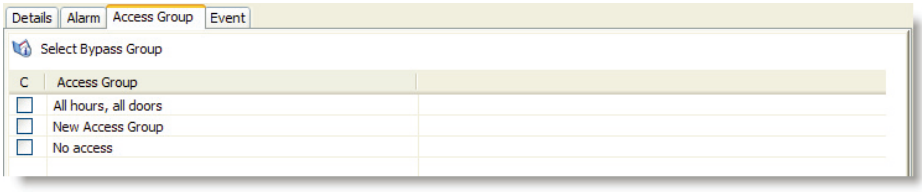
The Alarm tab allows you to specify alarm actions and an output device for an entrance limit zone.



- **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 3.9.1.2.
  - **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 3.9.2.
  - **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 Add at the bottom right of the Zone pane.

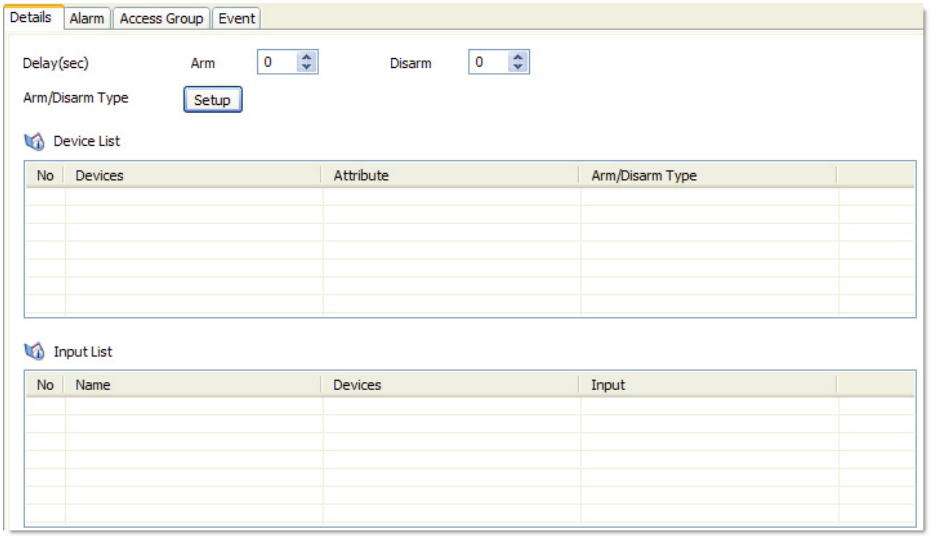


5.3.3 Customize Settings for Alarm Zones

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.

5.3.3.1 Details tab

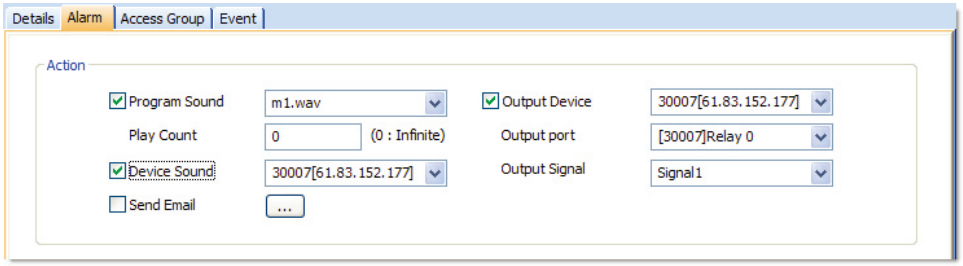
The Details tab allows you to specify alarm delays and arm/disarm types for alarm zones.



- **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 on setting up alarms, see section 3.9.

5.3.3.2 Alarm tab

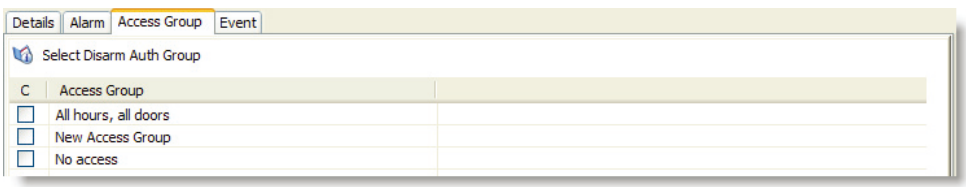
The Alarm tab allows you to specify alarm actions and an output device for an alarm zone.



- **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 3.9.1.2.
  - **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 3.9.2.
  - **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 **Add** at the bottom right of the Zone pane.

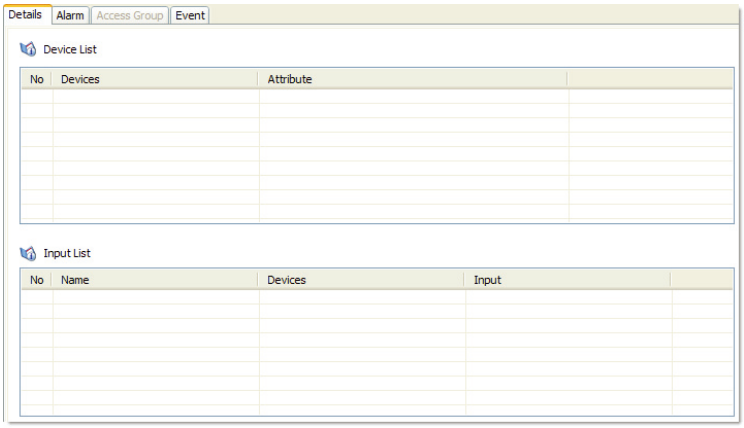


5.3.4 Customize Settings for Fire Alarm Zones

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.

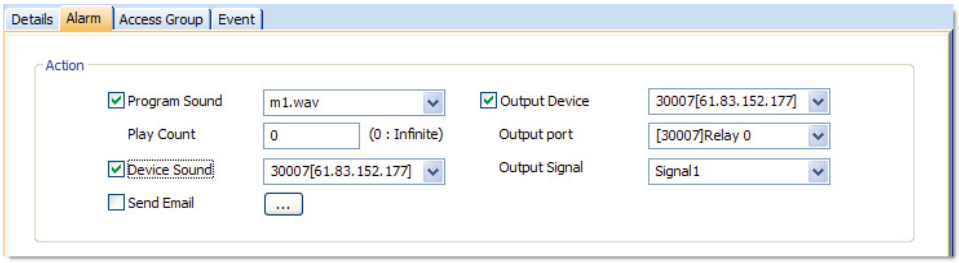
5.3.4.1 Details tab

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 3.4.2.2.



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 3.9.1.2.

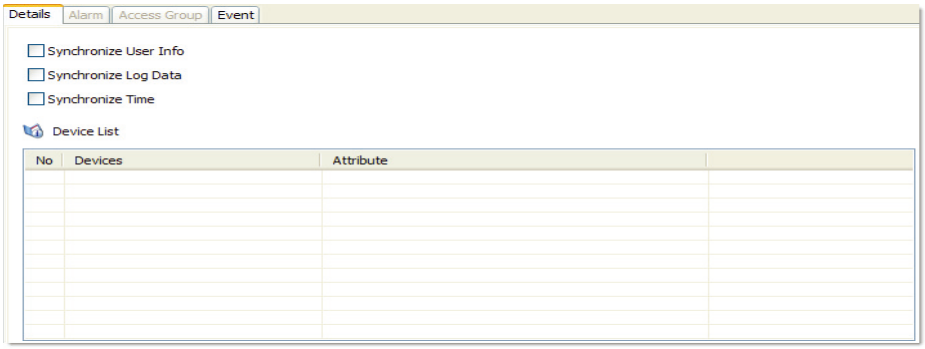
- **Device Sound** - activate and select a sound to be emitted by devices connected to the door.
- **Send Email** - activate and setup emails to be sent by the system. For more information about sending alert emails, see section 3.9.2.
- **Output Device** - activate and select a device to output an alarm 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.



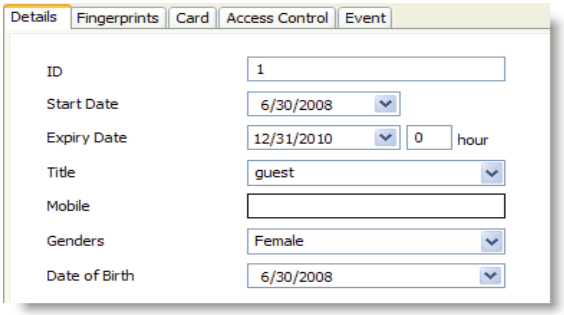
- **Synchronize User Info** - click this checkbox to automatically propagate user information to other devices.
- **Synchronize Log Data** - click this checkbox to automatically write all log records to the master device (for member devices in the zone).
- **Synchronize Time** - click this checkbox to synchronize the time of devices in the zone.

5.4 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

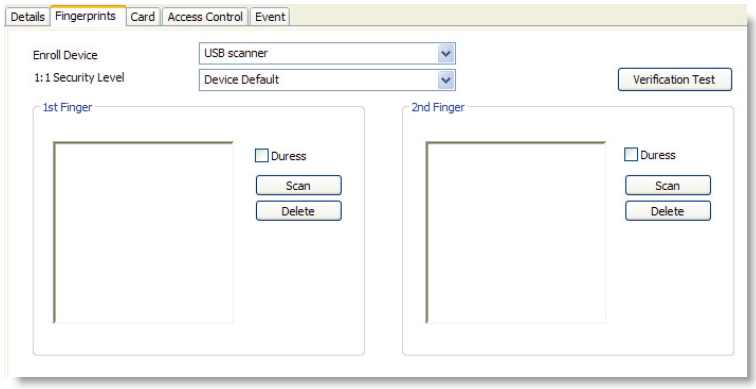
The Details tab allows you to specify personal information about a user and the valid dates of a user account. To edit these fields, see section 4.4.3.



- **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).
- **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.
- **Genders** - 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

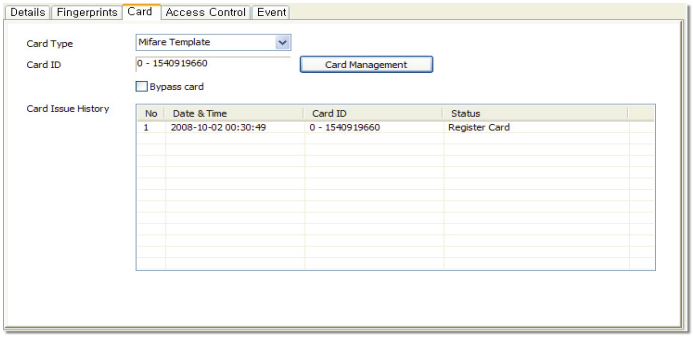
The Fingerprints tab allows you to specify which type of scanner to use for enrollment and the security level to apply. This tab can also be used to test for fingerprint matches and register duress fingerprints. For more information about registering fingerprints, see section 3.5.2.



- **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 Card Tab

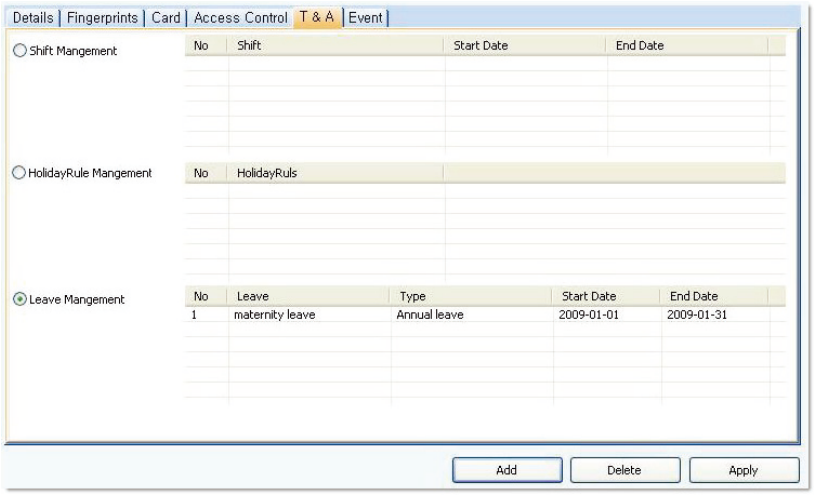
The Card tab allows you to specify card types and IDs and issue cards to users. For more information about issuing cards, see section 3.5.3.



- **Card Type** - select a type of access card to issue (*Mifare Card*, *EM 4100 Card*, or *HID Prox Card*).
- **Card ID** - displays the card ID number when a card is issued.

5.4.4 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, see section 3.8.



- **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 Solve Problems

If you experience problems with the BioStar software, contact Suprema's technical support by email: **support@supremainc.com**. When composing an email to technical support, please include the following:

- Which BioStar version you are using.
- Which Suprema devices are affected by the problem, if any.
- The error message you are receiving, if any.
- A complete (but concise) description of the problem you are experiencing.
- Your name and title.
- Your contact information.
- The best time and method to reach you

Glossary

access card - A card that can be used to grant or restrict access to a specific area. BioStar supports MIFARE®, EM4100, and HID proximity 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, BioEntry Plus, and SFR300 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).

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 devices support HID and EM4100 cards, while BioEntry Plus devices support EM4100 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 several zone classifications: anti-passback, entrance limitation, alarm, and fire alarm.

Index

Index

Index

suprema

BioStar

Suprema Inc.
16F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863 Korea

Tel : +82-31-783-4502, **Fax** : +82-31-783-4503
E-mail : sales@supremainc.com **Homepage** : www.supremainc.com