BioStar

Migration Guide

Version 1.0

Revision History

Rev No.	Issued date	Description
1.0	2008. Oct. 24	Initial Release

1 Overview

BioStar is an IP-based distributed security solution targeted at small-to-medium access control market. The first distinguishing feature of BioStar is that it does not need any controller. Each device can acts as a controller in addition to fingerprint reader. Another distinct feature of BioStar is its flexible connectivity options. If LAN is already set up, you only have to plug Ethernet cables to the devices. If Ethernet is not available, you can still use RS485 serial interface. Moreover, you can mix the two interfaces at will. As long as there is a communication path between two devices, Ethernet or RS485, they can be grouped into a zone and can be controlled as a logical unit.

In narrower meaning, BioStar refers to the software, which will replace BioAdmin. There are several reasons we have developed BioStar instead of upgrading BioAdmin. First of all, BioAdmin was not designed as a full-fledged access control software. Its initial goal was to provide basic user and device management functions. As more and more features have been integrated into it, its user interface and structure got more complex. Therefore, we decided to design a new software platform, on which we will be able to add new features such as time attendance in the future. We also redesigned operation flow from scratch to enhance usability.

This guide helps the users of BioAdmin migrate to BioStar. It presents an overview of the differences between the two software, from the points of view of both the system installer and operator, and then describes a process for performing a migration from BioAdmin to BioStar.

1.1 Why Migrate to BioStar?

BioStar has some important advantages over BioAdmin.

- ***Full-featured access control software***: BioAdmin has incorporated access control features on a rather ad-hoc basis. As a result, its user interface and operation flow get more and more convoluted with newer revisions. On the contrary, BioStar was designed as a full-featured access control software from the start. In addition to new powerful features such as alarm zone and server matching, BioStar provides much cleaner and well-organized user interface than BioAdmin.

- ***More powerful zone support***: High-level zone support has been incorporated since BioAdmin V4.2. However, there are some major constraints in configuring a zone. First of all, all the devices in a zone should be connected by LAN. The RS485 connection between devices is supported only for the single-door configuration. With BioStar, however, you can connect up to 8 devices through RS485 interface. As a result, you can easily replace legacy 4 or 8 door controllers with BioStar system. In addition to this, alarm zone and fire alarm zone are newly added. In combination with enhanced alarm management features, BioStar can provide the core functionality of intruder alarm system.

- ***Rich event/alarm management***: With BioAdmin, the available actions for alarm events are limited to writing logs and executing pre-defined functions. With BioStar, you can configure the alarm sound of devices or client PCs. E-mail messages can also be sent to the pre-defined addresses when alarm events occur.

- ***Flexible authentication mode***: The maximum number of enrolled user is limited by the capacity of each device. To bypass the limitation, server matching mode is introduced in BioStar. In server matching mode, user authentication is handled by BioStar server, not each device. Aside from extended capacity, this mode may be used when the fingerprint templates cannot be stored in devices for security reasons. Another enhancement is private authentication mode. You can fine-tune the authentication mode of each user in BioStar.

- ***Easy to install and use***: One of the major design goals of BioStar is to enhance usability by reorganizing its user interface. The GUI is categorized into 5 main menus – User, Door/Zone, Access Control, Monitoring and Device. Each menu has its own tree view, list view, and task list in a Microsoft Outlook-like interface. For complex operations such as device search and zone configuration, wizard interface is judiciously adopted. For easier installation, the express setup mode is added. In this mode, all the required software can be installed without users' intervention.

- ***Extensible***: BioStar is Suprema's integrated software platform for small-to-medium security market. In addition to access control, new functionalities such as time attendance will be incorporated in later versions. It can also handle much larger system than BioAdmin. By selecting BioStar now, you will be able to migrate seamlessly with the future enhancements of Suprema's security solutions.

1.2 Why Not Migrate to BioStar?

In some situations, migration is neither necessary nor desirable.

- ***All current needs are met by BioAdmin***: Migration to BioStar might not be a trivial task, especially if doors and zones of BioAdmin V4.2 are extensively used. If all your current needs are met by BioAdmin, you don't have to migrate. Please read Chapter 3 carefully before deciding whether to migrate.
- ***Time attendance***: As of V1.0, BioStar does not provide any time attendance functionality. Therefore, to use BioStation or BioEntry plus for time attendance applications, you have to use BioAdmin or develop your own applications using the BioStar SDK.
- ***Legacy devices***: BioEntry Smart/Pass and BEACon are not supported by BioStar. If these devices are already installed, the only option is to use BioAdmin.

2 BioAdmin vs. BioStar

This chapter describes the major differences between BioAdmin V4.2.x and BioStar V1.0. Its contents are not mandatory for the migration process. You can skip to Chapter 3 if you are to start the migration immediately.

2.1 Summary

<table>
<tr><td colspan="2" rowspan="2"></td><td rowspan="2">BioAdmin V4.2.x</td><td colspan="2">BioStar V1.0</td></tr>
<tr><td>Free Version</td><td>Standard Version</td></tr>
<tr><td colspan="2">Device</td><td>BioEntry Pass
BioEntry Smart
BEACon
BioStation
BioEntry Plus
BioLite Net[1]
Secure I/O</td><td colspan="2">BioStation(V1.5 or later)
BioEntry Plus(V1.2 or later)
BioLite Net[2]
Secure I/O</td></tr>
<tr><td colspan="2">Database</td><td>Access DB(default)
MS SQL Server
MySQL</td><td colspan="2">MS SQL Server Express(default)
MS SQL Server
MySQL</td></tr>
<tr><td rowspan="2">Capacity</td><td>Client</td><td>32</td><td>2</td><td>32</td></tr>
<tr><td>Door</td><td>128</td><td>20</td><td>512</td></tr>
<tr><td rowspan="2">RS485</td><td>To PC</td><td>Up to 31 devices</td><td colspan="2">Up to 31 devices</td></tr>
<tr><td>Devices</td><td>Up to 2 devices and 4 Secure I/Os</td><td colspan="2">Up to 8 devices (maximum 4 Secure I/Os)</td></tr>
<tr><td>User Management</td><td>Operator</td><td>3 pre-defined levels</td><td colspan="2">3 pre-defined levels
Custom levels can be created</td></tr>
</table>

[1] It will be supported in BioAdmin V4.3.

[2] It will be supported in BioStar V1.1.

	Private Authentication Mode	NA	Supported	
	Automatic Synchronization	NA	Supported	
	Search	NA	Supported	
	Group Change	NA	Supported	
	Server Matching	NA	NA	Supported
Zone	Maximum Device	32	NA	64
	Types	Anti-passback Entrance limitation	NA	Anti-passback Entrance limitation Alarm Fire alarm
	Constraints	All devices should be connected by LAN.	NA	At least one device should be connected by LAN.
Monitoring	Event Group	NA	5 Priority Levels	
	Event Notification	Log Output signal	Log Output signal Program sound Device sound	Log Output signal Program sound Device sound e-mail

Table 1. Differences between BioAdmin and BioStar

2.2 Zone

From the point of view of system installation, the biggest difference of BioStar is its flexibility in connecting devices for a zone. See Figure 1 for an example of zone configuration in BioStar. This section describes the general concept of zone configuration and explains the differences between BioAdmin and BioStar.

2.2.1 General Concepts

Master/Members in a Zone

Zones are used to group a number of devices to have a specific function. A zone consists of a master device, which plays a role similar to that of a legacy controller, and the other member devices. Both BioStation and BioEntry Plus can be a master device.

Host/Slaves in a RS485 network

In a half-duplex RS485 network, only one device should initiate all communication activity. We call this device ‘host’, and all the other devices ‘slaves’.

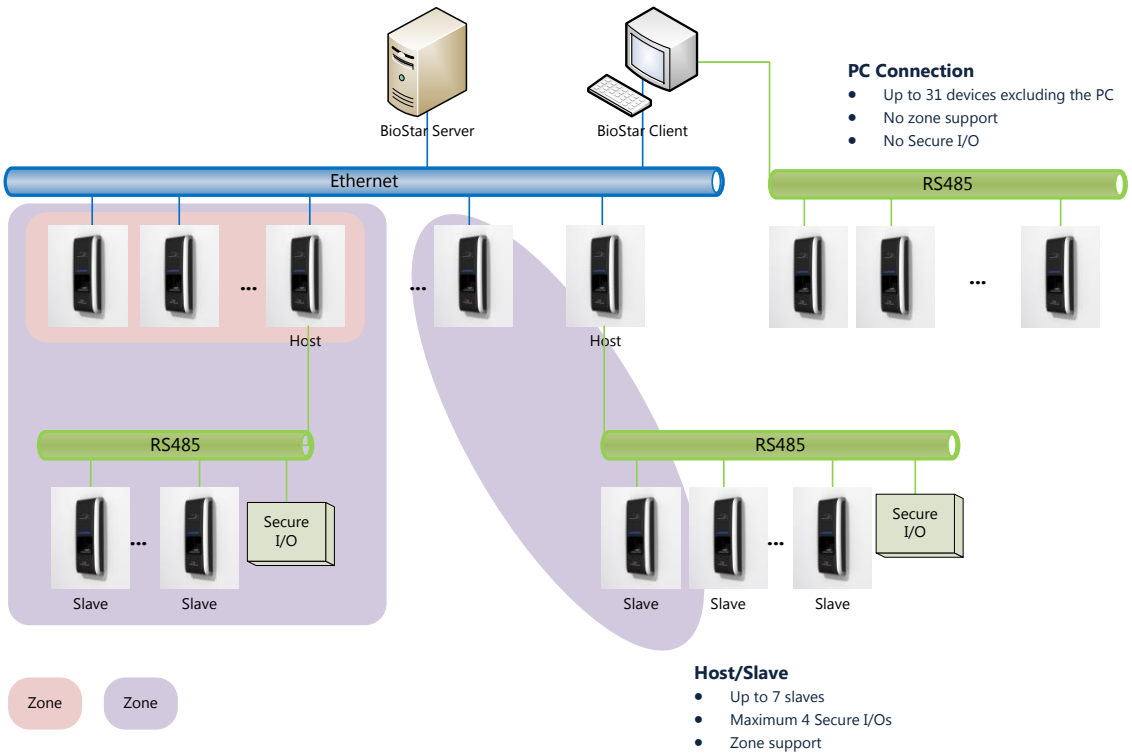

Figure 1. Zone Configuration of BioStar

2.2.2 RS485 Connection

Each BioStation or BioEntry Plus has one RS485 port, which can be used for connection to PC or other devices. The RS485 Mode setting of the device should be configured to one of the following modes;

- ***PC Connection***: The RS485 port is used for connecting to the PC. Maximum 31 devices can be connected to the PC through a RS485 network. In this case, the PC acts as the host device. Note that there is no zone support in this configuration.
- ***Host***: The device initiates all communication activity in a RS485 network. In terms of host, BioStar has two main advantages over BioAdmin.

  (1) The host device can control up to 7 slave devices including maximum 4 Secure I/Os. For example, a BioStation host may have 7 BioEntry Plus slaves, or 3 BioStation slaves and 4 Secure I/Os. In BioAdmin, it can control maximum 4 Secure I/Os and only one slave device.

  (2) The host device mediates packet transfers between the BioStar server and the slave devices. In other words, the BioStar can transfer data to and from the slave devices even when only the host device is connected to the PC thorough LAN. On the other hand, with BioAdmin, the slave device should be connected to the LAN for data transfer.
- ***Slave***: The slave device is connected to the host through RS485. It can communicate with BioStar through the host device.

There is another difference related to I/O configuration. In BioAdmin, the host device can control all the input and output ports of its own, Secure I/Os, and the slave device, while the slave cannot control even its own I/O ports. In BioStar, both the host and slave devices can control the ports of its own and Secure I/Os.

2.2.3 Zone Configuration

There are several differences between BioStar and BioAdmin in zone configuration.

- The maximum number of devices in a zone is increased to 64 from 32.
- Alarm and Fire Alarm zones are added.

- The only network constraint is that the master device should be connected to LAN. On the other hand, all member devices should be connected to LAN in BioAdmin.
- In BioAdmin, there are two steps for zone configuration. First, a generic zone is created with multiple devices. Then, a subzone with specific function such as anti-passback is created with a subset of the generic zone. In BioStar, the differentiation of zone and subzone is removed. You only have to create a zone with specific function. See Figure 2 for a visual description of this difference.

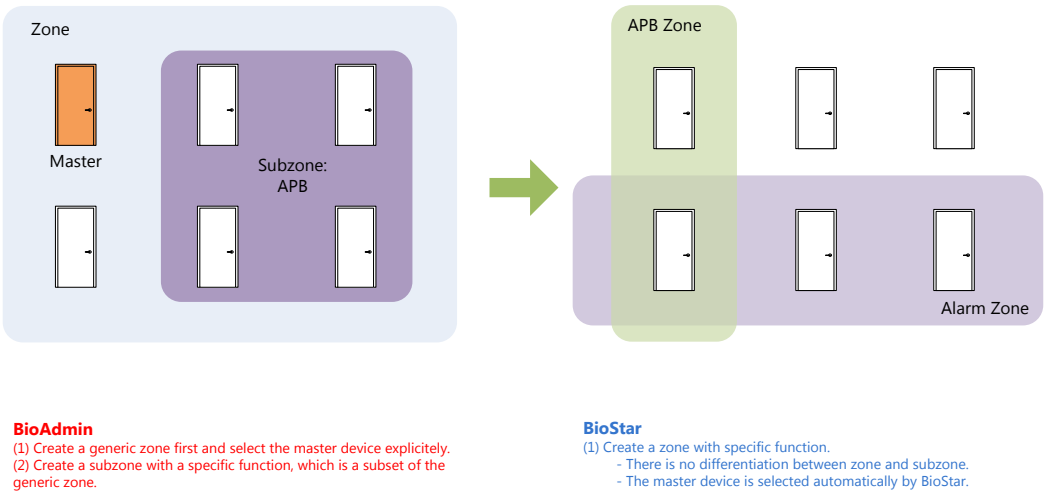

Figure 2. Zone Configuration Procedure

Please note that the zone configurations of BioAdmin and BioStar are not compatible. Refer to 3.2.7 for reconfiguration of zones.

2.3 Other Features

In addition to new zone support, BioStar has many enhancements over BioAdmin. This section describes major new features of BioStar in comparison with BioAdmin.

2.3.1 User Management

- You can define up to 4 levels of department, which can be used for grouping users. Department may be very useful when accessing the users of a specific group or changing the common settings of multiple users.
- User search function is added.
- Authentication mode can be set per user basis. For this setting to be effective, the **Private Auth** setting of **Device/Operation Mode** should be set to **Enable**.
- Automatic user transfer option is added. If **Option/User/Transfer Mode** is set to **Auto**, the changes of user information are transferred to the connected devices automatically.

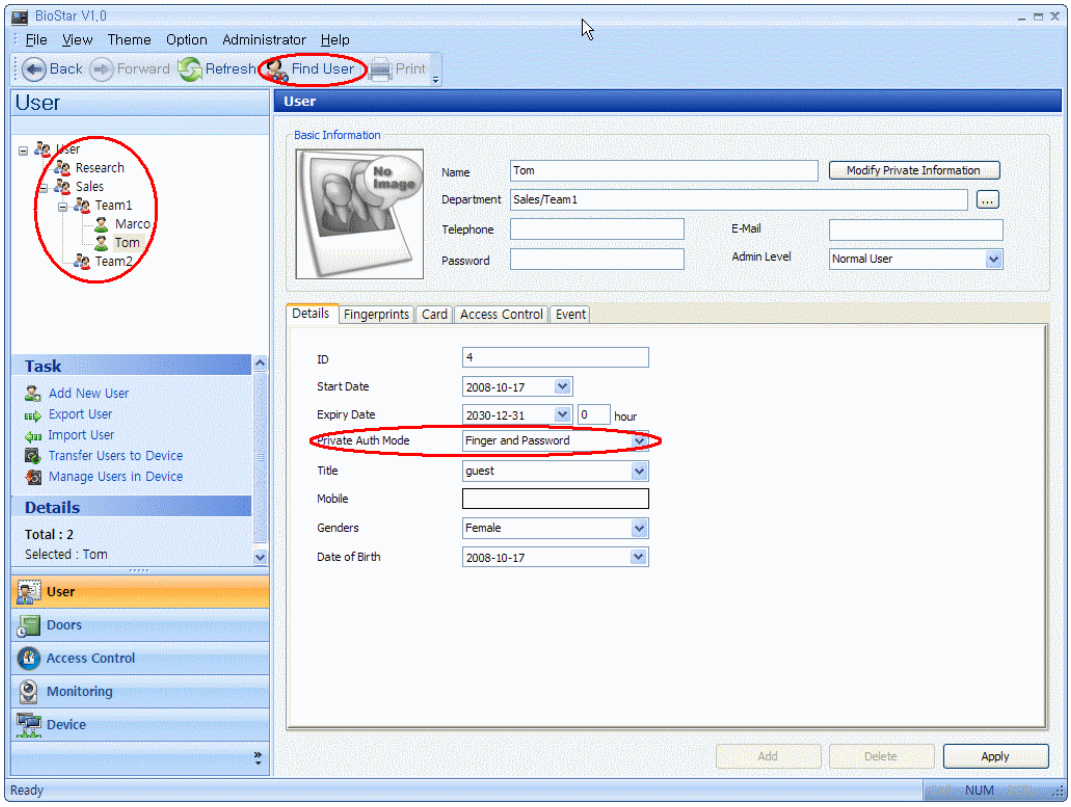

Figure 3. User Management

2.3.2 Door Management

In BioAdmin, you have to configure doors in the **Device Management/Door Setting** tab. In BioStar, the door menu becomes one of the five main menus. It is no longer subordinate to device configuration. On the contrary, most of access control features can be configured in door menu. We believe that this reorganization enhances usability and makes the interface more intuitive. There is one caveat, though. Like zone, the door configurations of BioAdmin and BioStar are not compatible. Refer to 3.2.6 for reconfiguration of doors.

2.3.3 Log Management

- Network Log is added. When you change the network settings of devices in BioStar, these activities are written into the BioStar server. These log records may be helpful for network troubleshooting process.
- Log filtering is enhanced. You can filter log records by door groups or 5 pre-defined priority levels.
- Real-time zone monitoring is added. You can monitor any alarm events of zones at the monitoring window.

2.3.4 Alarm Management

In addition to writing log records and sending output signals, three more actions can be configured for each priority group of alarm events.

- Sending e-mails to pre-defined addresses.
- Emitting alarm sounds through BioStation or BioEntry Plus devices.
- Emitting alarm sounds through BioStar clients.

2.3.5 Miscellaneous Features

- In addition to 3 pre-defined administrative levels, you can define custom levels to fine-tune the

privileges of operators.

- Server matching is supported. This mode has two important advantages.
  - Since the user information is stored in BioStar server, the capacity of users can be extended beyond the limit of each device.
  - The private information of each user can be protected more securely in the centralized BioStar server.
- Default encryption mode is added to BioStation. With BioAdmin, there is only one encryption mode – OpenSSL. And, by default, the communication packets are not encrypted. However, with BioStar, the communication packets are encrypted by default with an AES128 bit encryption algorithm. You can escalate the encryption mode to OpenSSL later.

3 Migration

Migration from BioAdmin to BioStar progresses in the following order.

(1) Upgrade firmware.

(2) Install BioStar.

(3) Convert the database of BioAdmin.

(4) Add devices to BioStar.

(5) Reconfigure devices if necessary.

(6) Reconfigure doors or zones if necessary.

Please note that you should not uninstall BioAdmin until the migration process finishes successfully. Otherwise, you might not be able to convert the database of BioAdmin.

The first four steps are rather straightforward. However, the last two steps might be tricky and requires detailed planning. You are strongly advised to read this chapter carefully before starting the migration process.

3.1 Checklist

The details of each step will vary according to your specific requirements. Below is a checklist to review before starting the migration process.

- ***Is the firmware of your devices compatible with BioStar?*** See Table 2 to check if your devices have the updated firmware. If not, you have to upgrade them first.
- ***What network interfaces are used for connecting devices?*** After installation of BioStar, you have to search the devices again manually. Therefore, you are strongly advised to write down the network settings of all the devices connected to BioAdmin.
- ***What is your database configuration in BioAdmin?*** If you use MS SQL Server or MySQL with BioAdmin and still want to use it with BioStar, you have to know the exact

settings of the database configuration.

- ***Do you want to run both BioAdmin server and BioStar server at the same PC?*** In some rare cases, it might be necessary to run both servers for test purpose. Since both servers use the same TCP port - 1480 - by default, you have to change at least one of them before or during the installation process.
- ***Are any devices connected by RS485?*** Since RS485 connection is not compatible between BioAdmin and BioStar, you have to reconfigure the setting. See 3.2.5 for details.
- ***Are any doors configured in BioAdmin V4.2.x?*** Since door configuration is not compatible between BioAdmin and BioStar, you have to reconfigure the doors. See 3.2.6 for details.
- ***Are any zones configured in BioAdmin V4.2.x?*** Since zone configuration is not compatible between BioAdmin and BioStar, you have to reconfigure the zones. See 3.2.7 for details.

3.2 Migration Process

3.2.1 Upgrade Firmware

To make use of the new features of BioStar, the firmware of the devices should meet the following requirements.

	BioStation	BioEntry Plus
Required Firmware Version	V1.5 or later	V1.2 or later

Table 2. Firmware Compatibility of BioStar

- You can upgrade firmware in BioStar after installation. However, to minimize any risk that might happen during the installation, we recommend that you upgrade firmware before the process.
- These newer versions of firmware are backward compatible. You can use them with BioAdmin

without any modification. For example, if you configure doors or zones in BioEntry Plus V1.0 or V1.1 with BioAdmin, these configurations will still work after upgrading the firmware to V1.2. This compatibility, however, will be broken as soon as you reconfigure the corresponding settings in BioStar.

3.2.2 Install BioStar

Below is a list of prerequisites for the installation process.

(1) Exit BioAdmin client applications if any.

(2) Stop the BioAdmin Server service in the BioAdmin Server Configuration utility or Windows Control Panel.

(3) If you use MS SQL Server or MySQL with BioAdmin and still want to use it with BioStar, you have to write down the following information.

A. The address and port number of the database server.

B. Authentication method and the proper credential to create new tables in the database.

For the detailed procedures of BioStar installation, please refer to 2 Install the BioStar Software of the *BioStar Administrator Guide*.

3.2.3 Convert the Database

After installing BioStar, you have to convert the user and log databases of BioAdmin to those of BioStar. We provide **BADV Conv** utility for this purpose. Refer to 2.6 Migrate a Database from BioAdmin to BioStar of the *BioStar Administrator Guide* for details. After conversion, you can use all the user and log data of BioAdmin in BioStar.

3.2.4 Add Devices to BioStar

You have to add devices to BioStar manually after installation. As long as the device is able to connect to BioAdmin, you can add it to BioStar with the same network settings. BioStar has several enhancements in

searching devices, too.

- You can search both BioStation(with firmware V1.5 or later) and BioEntry Plus through UDP. With this method, you can search all the devices of a subnet in one try.
- Range search is added for TCP. You can assign range of IP addresses to find multiple devices.

Refer to 3.2.1 Search for and Add Devices of the *BioStar Administrator Guide* for details.

3.2.5 Reconfigure Devices

As described in 2.2.2, the role of RS485 connection is greatly extended in BioStar. To accommodate this change, the configuration of RS485 is revised in BioStar. Even if the name of each mode is retained in BioStar, you have to reconfigure it for proper operation. The reconfiguration procedure will vary according to the old **Device Configuration/Network Setting/RS485/ Mode** in BioAdmin.

Disabled

You don't have to reconfigure anything.

PC Connection

The PC connection will work with the same baudrate specified in BioAdmin. However, it will be shown as Disabled for BioStation in BioStar. To prevent further confusion, you had better change **Device/Network/RS485/Mode** setting to **PC Connection** and press **Apply** before changing any other settings.

Host

You have to change **Device/Network/RS485/Mode** setting to **Host** in BioStar.

(1) If you have Secure I/Os connected to the device through RS485

A. Right-click the device at the device tree and select **Add Device(Serial)**.

B. Search and add the Secure I/Os. See 3.2.2 Search for and Add Slave Devices in the *BioStar Administrator Guide*.

C. Reattach the Secure I/Os to the host by pressing the SYNC button on the front panel of Secure I/Os for a few seconds.

(2) If you have a slave device,

A. Change the **Device/Network/RS485/Mode** setting of the slave device to **Slave**. Then, remove it from the device tree.

B. Search and add the slave device with the same process as above.

C. If you configured any I/O ports of the slave device in BioAdmin, you have to reconfigure them under the I/O settings of the slave device.

Slave

You have to change **Device/Network/RS485/Mode** setting to **Slave** in BioStar. See the above paragraph for adding the slave device to the host.

3.2.6 Reconfigure Doors

The door configurations of BioAdmin and BioStar are not compatible. You have to reconfigure door settings in BioStar. There are several differences related to door configurations.

- While the door setting is a sub menu of device management in BioAdmin, it is one of 5 main menus in BioStar. You have to create a door first, and then add up to two devices to it.
- When two devices are added to one door, both of them should be connected by the same RS 485 network. The two devices can be either a host or a slave. And the ports of only one device can be used for door settings.
- Door group is supported. It is useful for managing and monitoring related doors in a group.
- There is no **Two Door** mode in BioStar. The similar effect can be achieved by combining the door configuration with I/O settings.

Refer to 3.3 Setup Doors in the *BioStar Administrator Guide* for the detailed descriptions of each setting.

3.2.7 Reconfigure Zones

You cannot use the zone configurations of BioAdmin in BioStar. Even if you are to use the same type of zone such as anti-passback, you have to reconfigure it in BioStar.

Converting anti-passback or entrance limitation zones of BioAdmin to BioStar is rather straightforward.

- Even slave devices can join a zone in BioStar. On the contrary, only the devices connected to LAN can join in BioAdmin.
- You can define bypass groups, the members of which are not constrained by the restriction of the zone. With BioAdmin, only the administrators are exempt from the constraints.

Refer to 3.4 Setup Zones in the *BioStar Administrator Guide* for the detailed configurations.

