

# Table of Contents

How to configure an Anti-Passback (APB) Zone? .....	1
Configuring a Local Anti-Passback Zone .....	1
Configuring the Anti-Passback Zone .....	2
Video Demo .....	6

[System Configuration](#), [BioStar 2](#), [APB](#), [Anti-passback](#), [Zone](#)

## How to configure an Anti-Passback (APB) Zone?

### Configuring a Local Anti-Passback Zone

For local anti-passback, you do not need an AC license. Follow the steps below to configure a local APB.

1. Add a master device to BioStar 2 in the **DEVICE** menu.
2. Add a slave device to the master device in the **DEVICE** menu with a RS485 connection.

Refer to [How to add devices](#) to learn how to add master and slave devices.

3. Click on the **DOOR** menu.
4. Click **ADD DOOR**.
5. Select your **Entry Device**.
6. Select your **Exit Device**.

Anti-Passback tab will appear when you add the exit device.

7. Configure the **Door Relay**, **Exit Button**, **Door Sensor** as necessary.
8. On the **Anti PassBack** tab, select type to **Hard**.

Soft Anti-Passback records logs but allows user entry on anti-passback violation.  
Hard Anti-Passback records logs and does not allow user entry on anti-passback violation.

9. On **Reset Time**, set the time when the anti-passback violation will be reset (after # of minutes).
10. Click **Apply** to apply the settings.

**Configuration**

- Entry Device: BioStation 2 546832586 (192.168.16.215)
- Exit Device: BioEntry W2 544108052
- Door Relay(s): Relay 0 of BioStation 2 546832586 (192.168.16.215) Device
- Exit Button: Input Port 0 of BioStation 2 546832586 (192.168.16.215) Device
- Door Sensor: Input Port 1 of BioStation 2 546832586 (192.168.16.215) Device
- Switch: Normally Open
- Switch: Normally Open

**Option**

Open

- Open Time: 3 sec
- Lock when door is closed: OFF
- Use Automatic Door: OFF

Dual Authentication

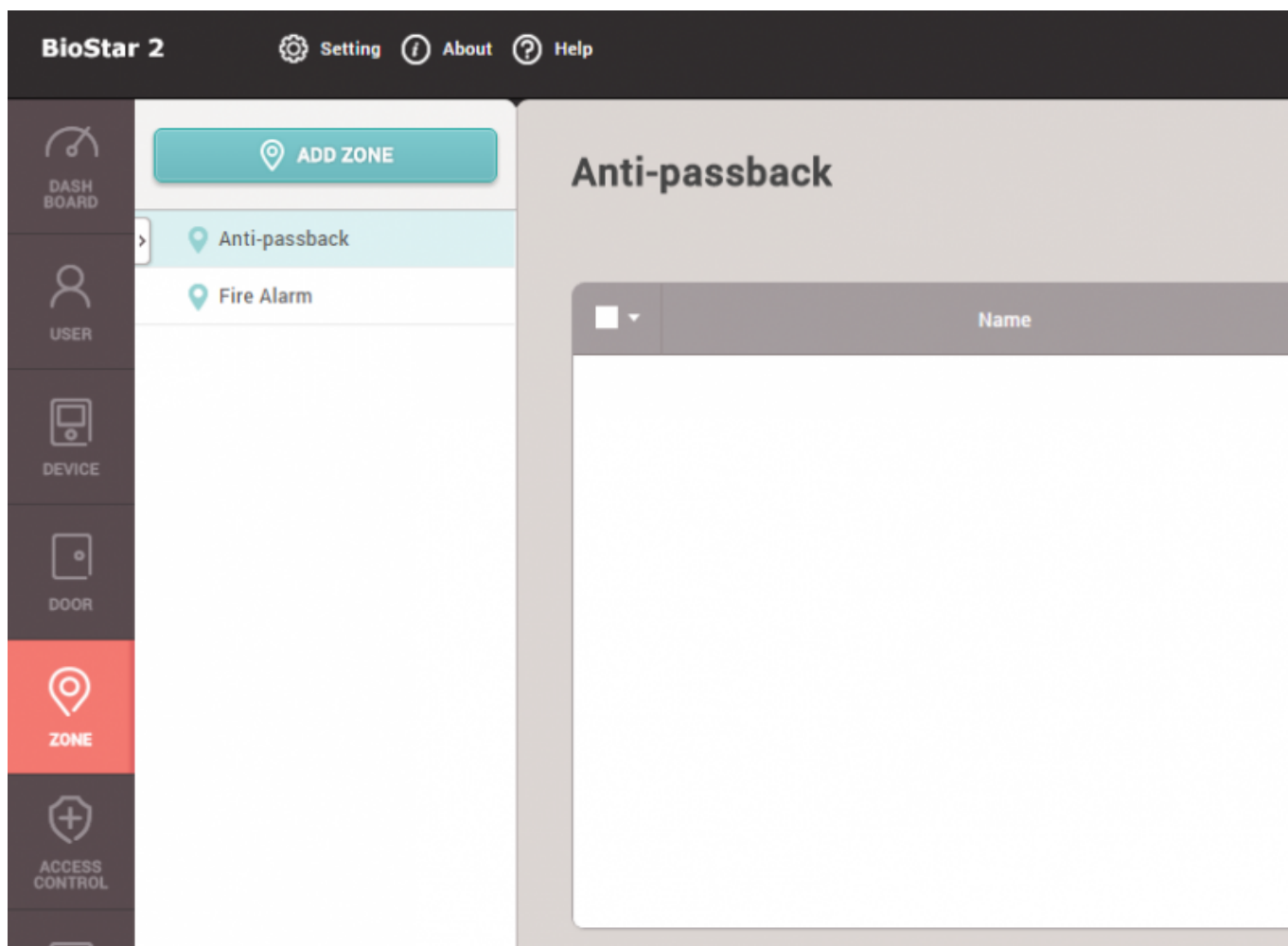
- Device: No device

**Anti PassBack**

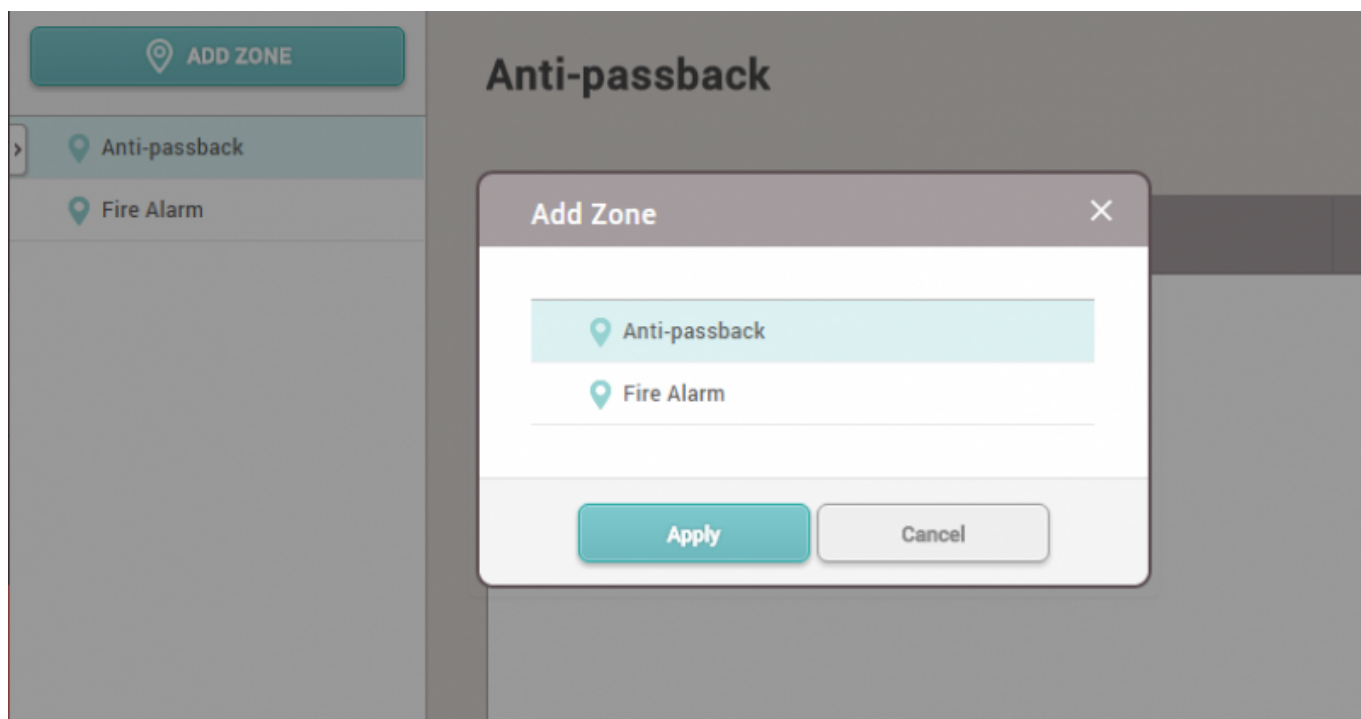
- Type: Hard APB
- Reset Time: 1440 min.

## Configuring the Anti-Passback Zone

Before you start, check the license activation status. If a standard edition is activated, the 'Zone' tap can be seen from the left menu buttons as below.



1. Click **ADD ZONE** and select **Anti-passback** and click **Apply**.



2. Enter the name of the APB zone, and make configuration as desired. If you want to block users who violate the APB rule, set the type to **Hard APB** and check **Reset Time** not to be shorter than the expected duration of the block time. And set **Entry Devices** and **Exit Devices**.

### Information

• Name

my APB

• Type

Anti-passback

### Configuration

• Mode

☒ Global

• Active/Inactive

☒ Active

• Anti-passback Type

☐ Hard APB

• Reset Time

1440 min.

• Entry Devices

BioStation A2 93925... ▼

• Exit Devices

BioStation L2 54008... ▼

• Network Failure Action

Open by auth ▼

For a ethernet based zone, select **Global** for the **Mode**. The server will be the master device making anti-passback decisions.

When choosing the **Global** mode you have the option to select a network failure action. If the device cannot communicate with the server, it will operate based on your configured action.  
Refer to the administrator's manual (help menu) for details.

3. Set an action if needed to make an alarm sound using the device relay.

The 'Add Action' dialog box is shown with a close button (X) in the top right corner. It contains a section titled 'Action' with four radio button options: 'Output' (selected), 'Release All Alarm', 'Reboot Device', and 'Disable Device'. To the right of these options are three dropdown menus: 'Device' (set to 'BioLiteNet 538101264'), 'Output' (set to 'Relay 0'), and 'Signal' (set to 'test'). At the bottom of the dialog are two buttons: 'Apply' (highlighted in teal) and 'Cancel'.

4. Set the APB Bypass group who will enter the doors in the APB zone regardless of the APB rule. It's recommended to be used for the admin users for the convenient fix and revision at the site.

The 'APB Bypass' section is shown with a header bar. Below the header, there is a label 'Bypass Group' with a red asterisk. To its right is a search dropdown menu. The dropdown menu is open, showing a search bar with the text 'Test' and a magnifying glass icon. Below the search bar, there is a list item 'Test' with a checked checkbox to its left.

5. After finishing the setting, test the APB and check alert and the zone status from monitoring.

The screenshot shows a 'Zone Status' interface with a table of zones. A modal window titled 'ACCESS\_DENIED\_APB' is open, displaying details of an anti-passback violation.

	Type	Zone Name	Active/Inactive	Status
<input type="checkbox"/>	Anti-passback	Test	Active	Normal

**ACCESS\_DENIED\_APB** [Close]

- User: Administrator
- Device: BioStation 2 100000007 (192.168.16.205)
- Alarm: Violation of anti-passback
- Date: 2015/09/16 16:46:18

Comments

**Acknowledge** **Ignore**

## Video Demo

[apb.mp4](#)

From:

<https://kb.supremainc.com/knowledge/> -

Permanent link:

[https://kb.supremainc.com/knowledge/doku.php?id=en:how\\_to\\_configure\\_apb\\_zone](https://kb.supremainc.com/knowledge/doku.php?id=en:how_to_configure_apb_zone)

Last update: **2021/12/20 10:16**