

## Tabla de Contenidos

¿Cómo configurar una zona Anti-Retorno (APB)? .....	1
Configuración de una Zona Anti-Retorno local .....	1
Configuración de una Zona Anti-retorno .....	2
Video de demostración .....	6

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

## ¿Cómo configurar una zona Anti-Retorno (APB)?

### Configuración de una Zona Anti-Retorno local

Para el anti-retorno local, no se necesita la licencia CA. Siga los pasos que se indican a continuación para configurar una zona anti-retorno local.

1. Agregue un dispositivo maestro a BioStar 2 en el menú **DEVICE**.
2. Agregue un dispositivo esclavo al dispositivo maestro en el menú **DEVICE** con una conexión RS485.

Consulte [Cómo agregar dispositivos](#) para aprender a agregar dispositivos maestros y esclavos.

3. Clic en el menú **DOOR**.
4. Clic en AGREGAR **DOOR**.
5. Seleccione su **Entry Device**.
6. Seleccione su **Exit Device**.

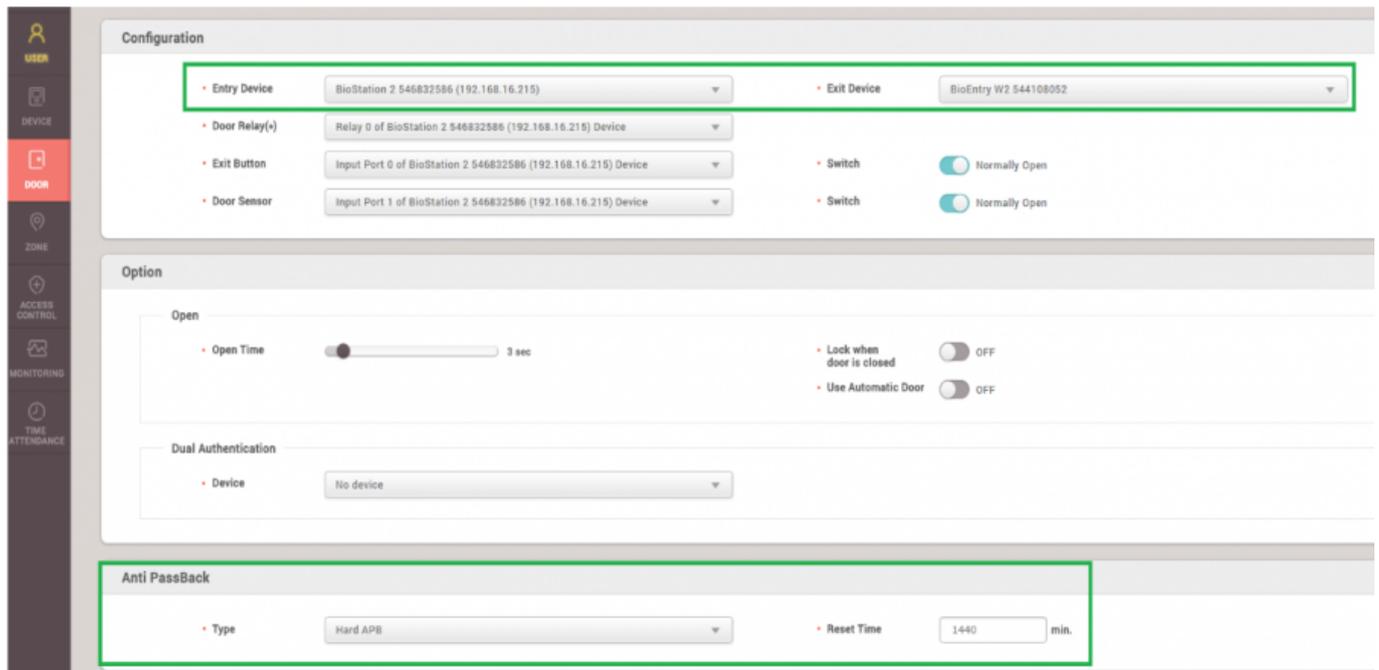
La pestaña Anti-retorno aparecerá cuando agregue el dispositivo de salida.

7. Configure el **Door Relay**, el **Exit Button**, el **Door Sensor** según sea necesario.
8. En la pestaña **Anti-Passback**, seleccione el tipo en **Hard**.

El Anti-retorno No estricto graba los registros, pero permite la entrada del usuario con infracción de Anti-retorno.

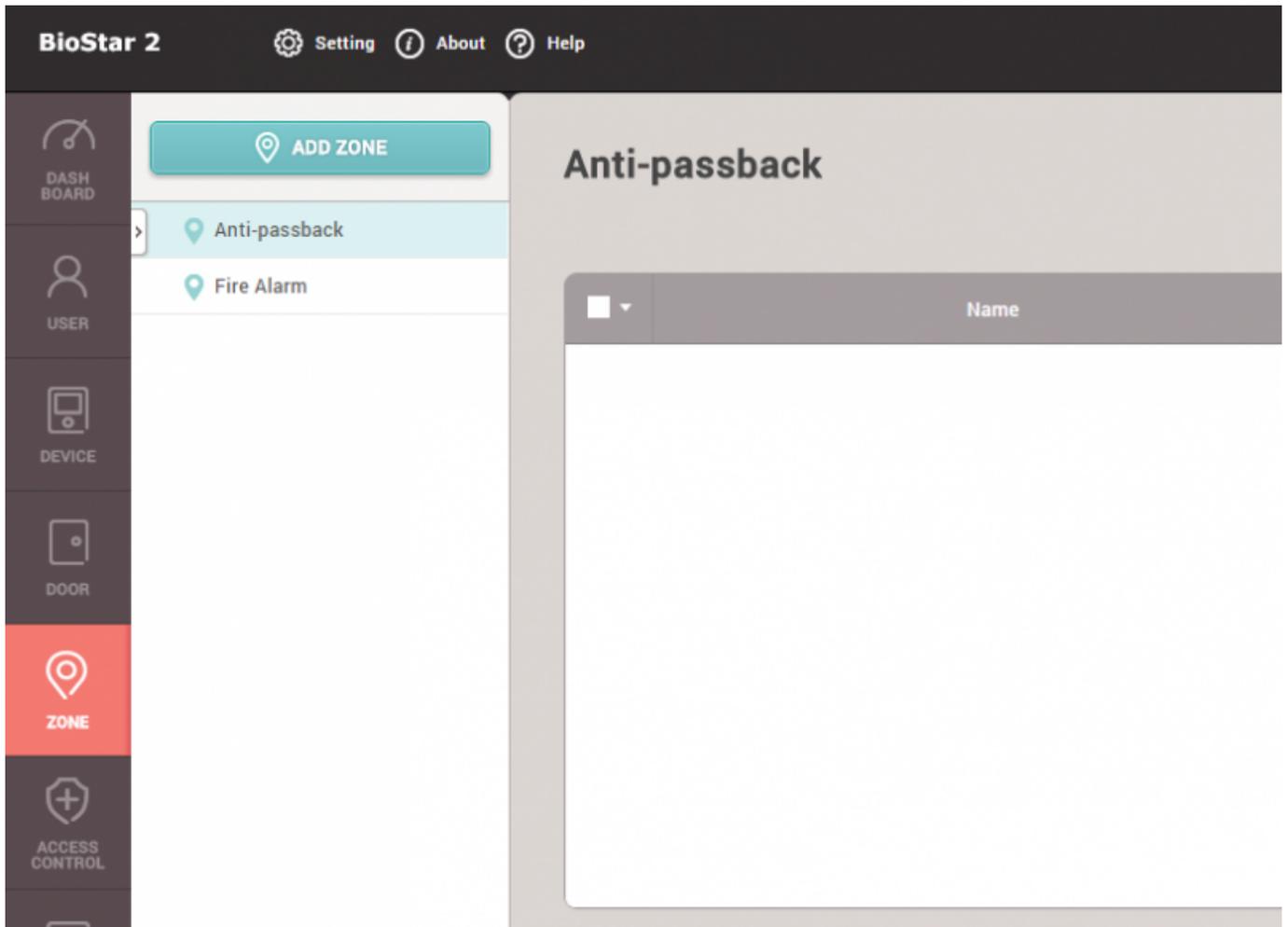
El Anti-retorno Estricto graba los registros, y NO permite la entrada del usuario con infracción de anti-retorno.

9. En **Reset Time**, fije la hora en la que se borrarán las infracciones de anti-retorno (después de # minutos).
10. Clic en **Apply** para aplicar los ajustes.

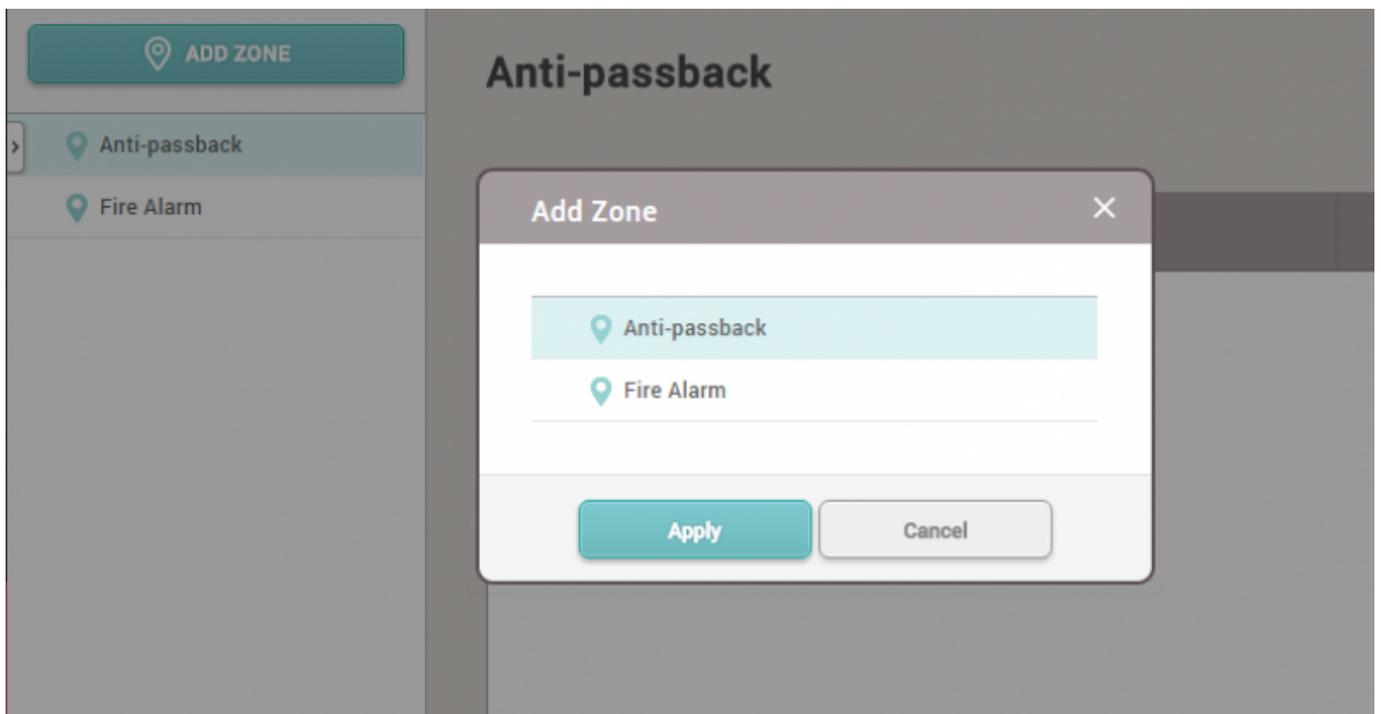


## Configuración de una Zona Anti-retorno

Antes de empezar, compruebe el estado de activación de la licencia. Si la edición estándar está activada, el icono 'Zona' se puede ver desde los botones del menú izquierdo como se muestra a continuación.



1. Haga clic en **ADD ZONE**, seleccione **Anti-passback** y haga clic en **Apply**.



2. Ingrese el nombre de la zona anti-retorno y haga los ajustes que desee. Si desea bloquear a los usuarios que infringen la regla del anti-retorno, seleccione **Hard APB** y marque **Reset Time** para que no sea más corto que la duración esperada del tiempo de bloqueo. Y establezca **Entry Devices** y **Exit Devices**.

### Information

• Name	<input type="text" value="my APB"/>	• Type	<input type="text" value="Anti-passback"/>
--------	-------------------------------------	--------	--

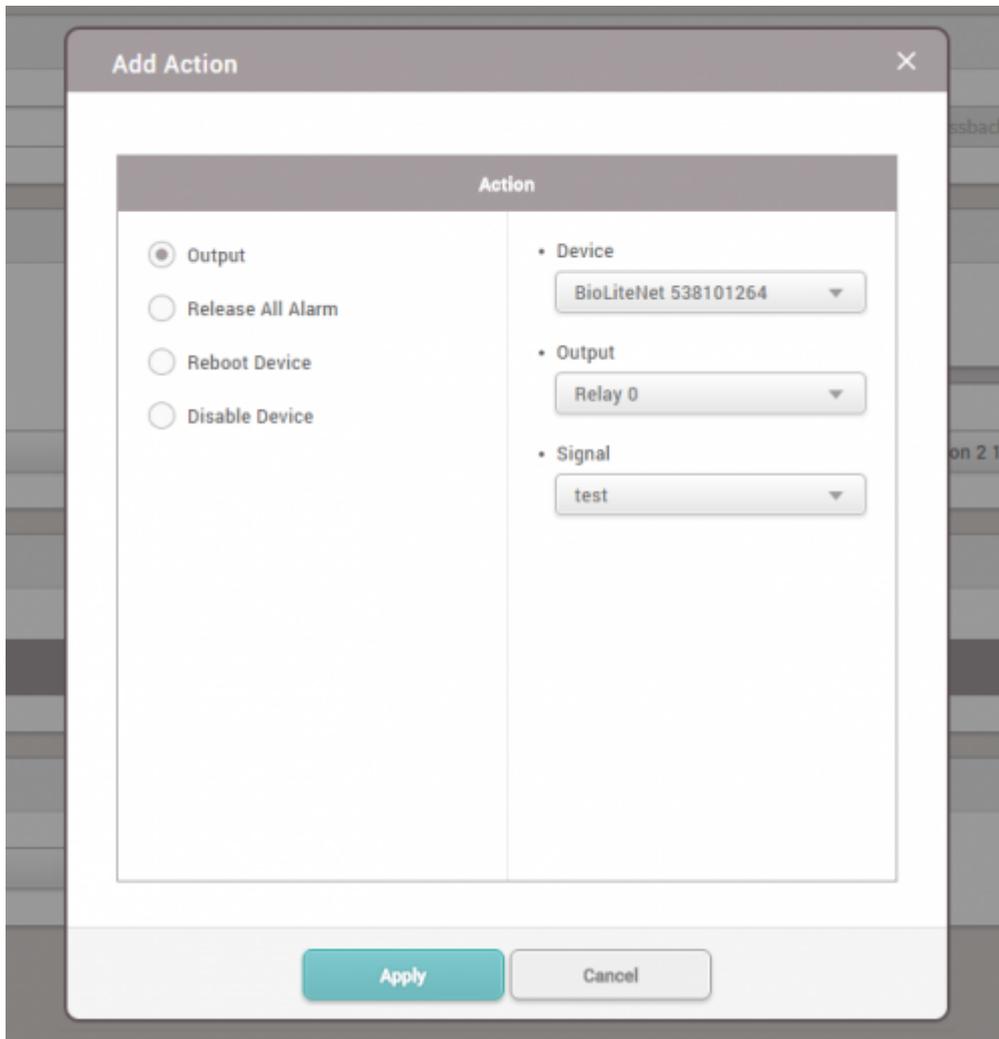
### Configuration

• Mode	<input checked="" type="checkbox"/> Global	• Active/Inactive	<input checked="" type="checkbox"/> Active
• Anti-passback Type	<input type="checkbox"/> Hard APB	• Reset Time	<input type="text" value="1440"/> min.
• Entry Devices	<input type="text" value="BioStation A2 93925..."/>	• Exit Devices	<input type="text" value="BioStation L2 54008..."/>
• Network Failure Action	<input type="text" value="Open by auth"/>		

Para una zona basada en Ethernet, seleccione **Global** en el **Mode**. El servidor será el dispositivo maestro que toma decisiones anti-retorno.

Al elegir el modo **Global**, tiene la opción de seleccionar una acción de error de red. Si el dispositivo no puede comunicarse con el servidor, funcionará según la acción configurada. Consulte el manual del administrador (menú de ayuda) para obtener más información.

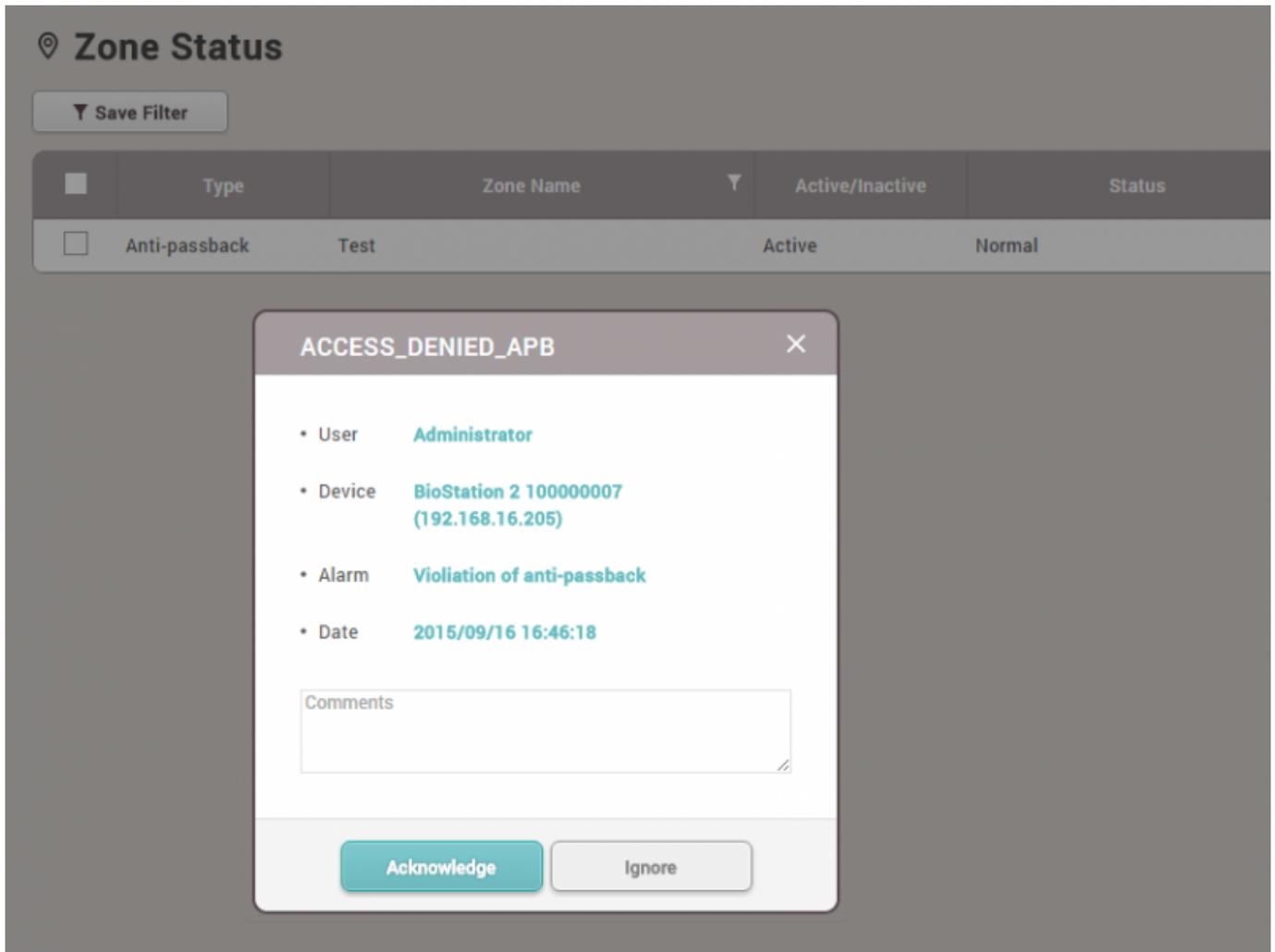
3. Si es necesario, establezca una acción para producir un sonido de alarma usando el relé del dispositivo.



4. Establezca el grupo de Elusión (bypass) de Anti-retorno que ingresará por las puertas en la zona de anti-retorno independientemente de la regla de anti-retorno. Se recomienda que los usuarios administradores lo usen para reparaciones y revisiones convenientes en el sitio.



5. Después de finalizar la configuración, pruebe el anti-retorno y compruebe el estado de la alerta y de la zona desde Monitoreo.



The screenshot displays the 'Zone Status' interface. At the top, there is a 'Save Filter' button. Below it is a table with columns: 'Type', 'Zone Name', 'Active/Inactive', and 'Status'. A single row is visible with the following data: 'Anti-passback', 'Test', 'Active', and 'Normal'. A modal window titled 'ACCESS\_DENIED\_APB' is open in the foreground, showing details of an alarm:

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

Below the details is a 'Comments' text area and two buttons: 'Acknowledge' and 'Ignore'.

## Video de demostración

[apb.mp4](#)

From:  
<http://kb.supremainc.com/knowledge/> -

Permanent link:  
[http://kb.supremainc.com/knowledge/doku.php?id=es:how\\_to\\_configure\\_apb\\_zone](http://kb.supremainc.com/knowledge/doku.php?id=es:how_to_configure_apb_zone)

Last update: **2020/12/08 14:41**