

# Tabla de Contenidos

Cómo configurar el seguro contra alteraciones (Tamper) .....	1
Configuración .....	1
Caso 1: .....	2
Caso 2: .....	3

## Cómo configurar el seguro contra alteraciones (Tamper)

Si el dispositivo se separa del soporte (se activa un evento) que eliminará rápidamente la información de todos los usuarios, registros, claves de cifrado y certificados SSL configurados en el dispositivo.

Dispositivo compatible:

Device	Version
BioStation 2	V1.6.0 or above
BioStation A2	V1.5.0 or above
CoreStation	V1.1.0 or above
BioEntry P2	V1.1.0 or above
BioStation L2	V1.4.0 or above
BioEntry N2	V1.0.0 or above
BioEntry W2	V1.2.0 or above
FaceStation 2	V1.1.0 or above

\* Entry device which firmware version is V2.x is not supported

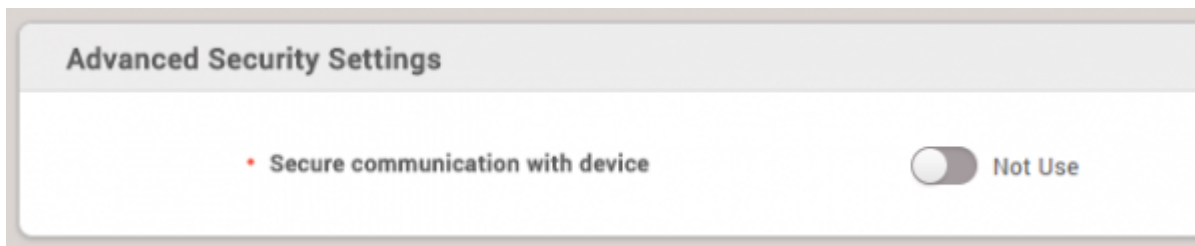
- Una vez generado el evento **Contra alteraciones(Tamper On)**, los usuarios guardados en BioStar 2 ya no se pueden sincronizar con el dispositivo. En este caso, se debe transferir usuarios al dispositivo manualmente.
- El dispositivo esclavo no es compatible.

### Configuración

Se presentan dos casos para configurar.

### Caso 1:

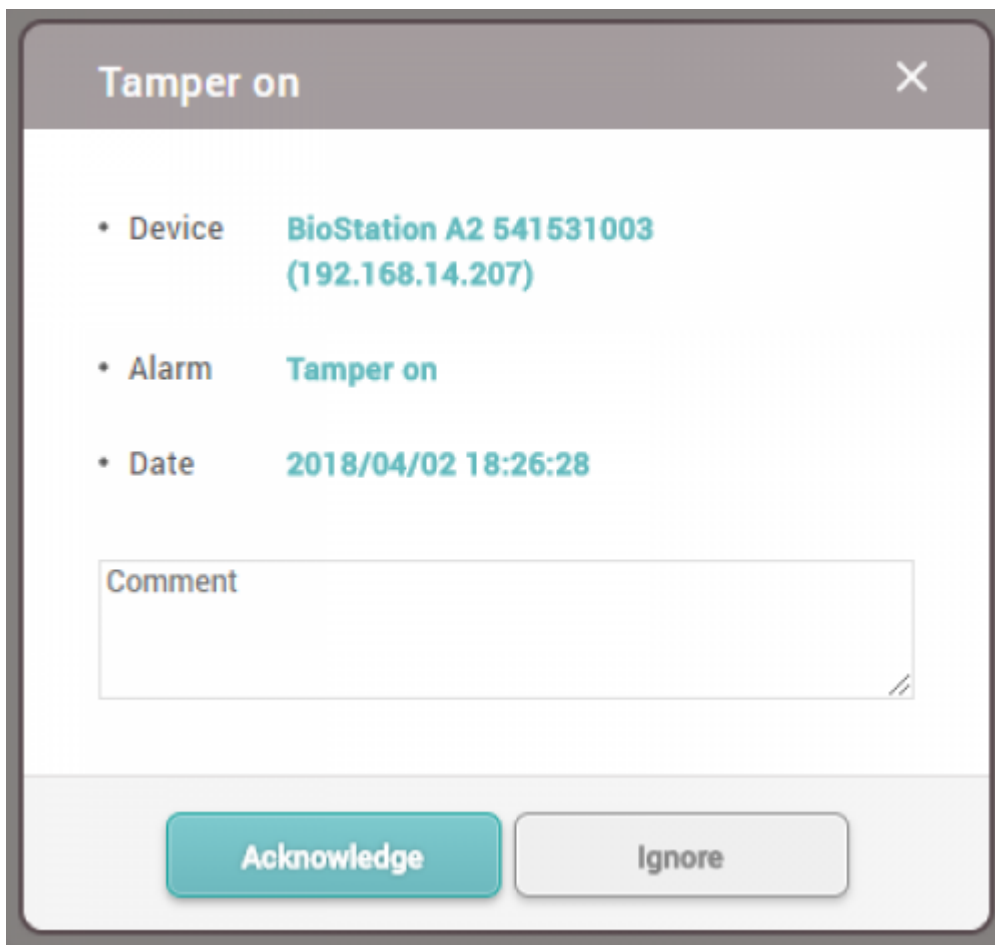
Si no Activa la **Comunicación segura con el dispositivo(Secure communication with device)** en **Ajustes(Setting) > SERVIDOR(SERVER)**, siga las instrucciones siguientes para configurar el Seguro contra alteraciones.



1. Vaya a **Ajustes(Setting) > Avanzado(Advanced)**
2. Cambie **Seguro contra alteraciones(Secure Tamper)** a **habilitado(On)**.



3. Cuando ocurre el evento **Contra alteraciones(Tamper)**, aparece el siguiente mensaje en BioStar 2.



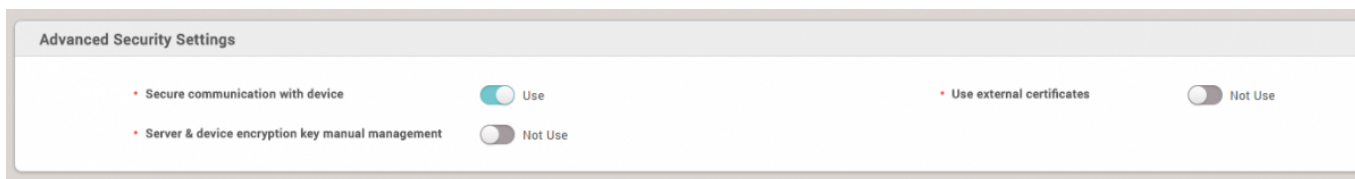
Entonces podrá ver los siguientes registros de eventos en la sección Monitoreo. En especial, si

comprueba los usuarios y los registros en el dispositivo directamente, se eliminarían por completo.

Date	Door	Elevator	Device ID	Device	User	Zone	Event	View
2018/04/02 18:29:47			541531003	BioStation A2 5...			Device Disconnection Detected	
2018/04/02 18:29:46			541531003	BioStation A2 5...			Database Reset	
2018/04/02 18:29:46			541531003	BioStation A2 5...			Tamper on	
2018/04/02 18:29:46			541531003	BioStation A2 5...			Event log cleared	
2018/04/02 18:29:45			541531003	BioStation A2 5...			Tamper on	
2018/04/02 18:29:45			541531003	BioStation A2 5...			Tamper off	


### Caso 2:

Si **Activa(Use)** la **Comunicación segura con el dispositivo(Secure communication with device)** en **Configuración(Setting) > SERVIDOR(SERVER)**, verá las opciones adicionales a continuación. Consulte **Administración manual de claves de cifrado de servidor y dispositivo(Server & device encryption key manual management)**.



Si **Activa(Use)** la **Administración manual de la clave de cifrado de servidor y dispositivo(Server & device encryption key manual management)**, verá el siguiente mensaje de advertencia. Tenga en cuenta que, si activa esta opción, la función **Seguro contra alteraciones(Secure Tamper)** se aplicará automáticamente. Tenga cuidado antes de aplicar este ajuste.

**Warning** ✕



**\*Cautions\***

- Please make sure to read the manual before enabling this function.
- Once enabled, please note that the device function of deleting users, logs, and encryption key at a tamper event is activated in order to increase the security.
- Manual key management cannot be applied when users except administrator have login PW and PIN. Please delete login PW and PIN before applying. This is because PW and PIN adopted undecodable encryption method to meet the regulation requirements.

**Ok**

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

Permanent link:  
[https://kb.supremainc.com/knowledge/doku.php?id=es:how\\_to\\_configure\\_secure\\_tamper](https://kb.supremainc.com/knowledge/doku.php?id=es:how_to_configure_secure_tamper)

Last update: **2020/03/03 17:54**