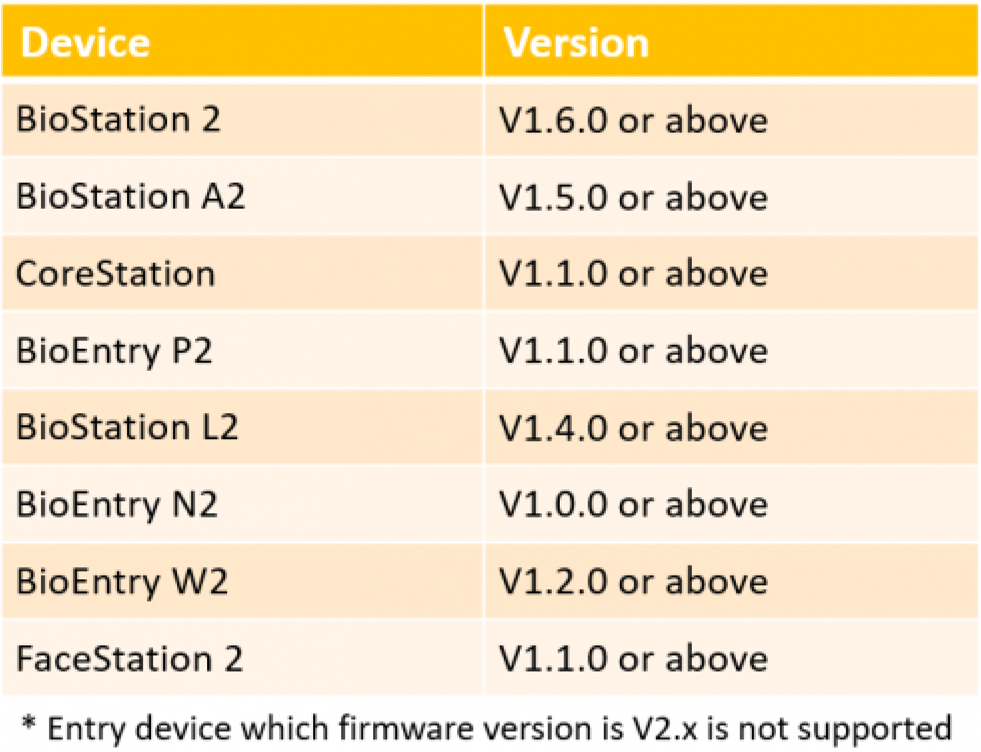
Table of Contents

How to configure Secure Tamper

If the device is separated from the bracket (**Tamper On** event happens), the information on all users, logs, encryption key and SSL certificates configured in the device will be deleted promptly.

Supported device:



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

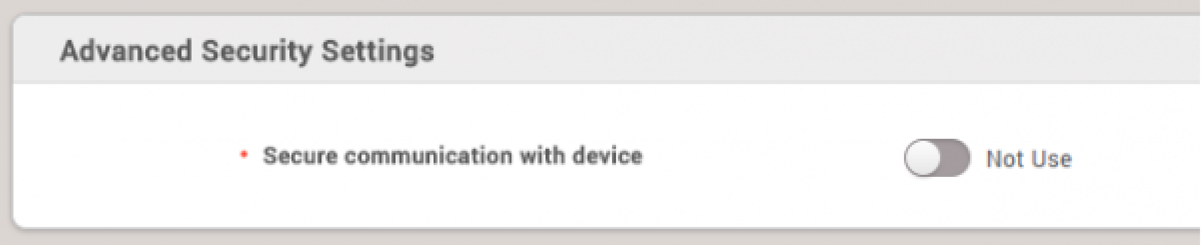
- Once the **Tamper On** event is generated, the users saved in BioStar 2 cannot be no longer synchronized with the device. In this case, you should transfer users to the device manually.
- Slave device is not supported.

How to configure

There are two cases to configure.

Case 1:

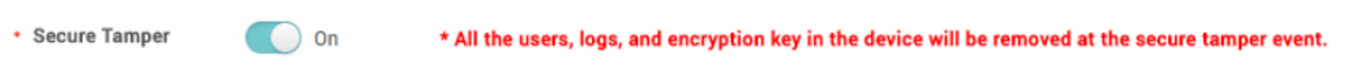
If you do not set **Secure communication with device** to **Not Use** in **Setting** > **SERVER**, you should follow below instructions to configure secure tamper.



Advanced Security Settings

* Secure communication with device — Not Use

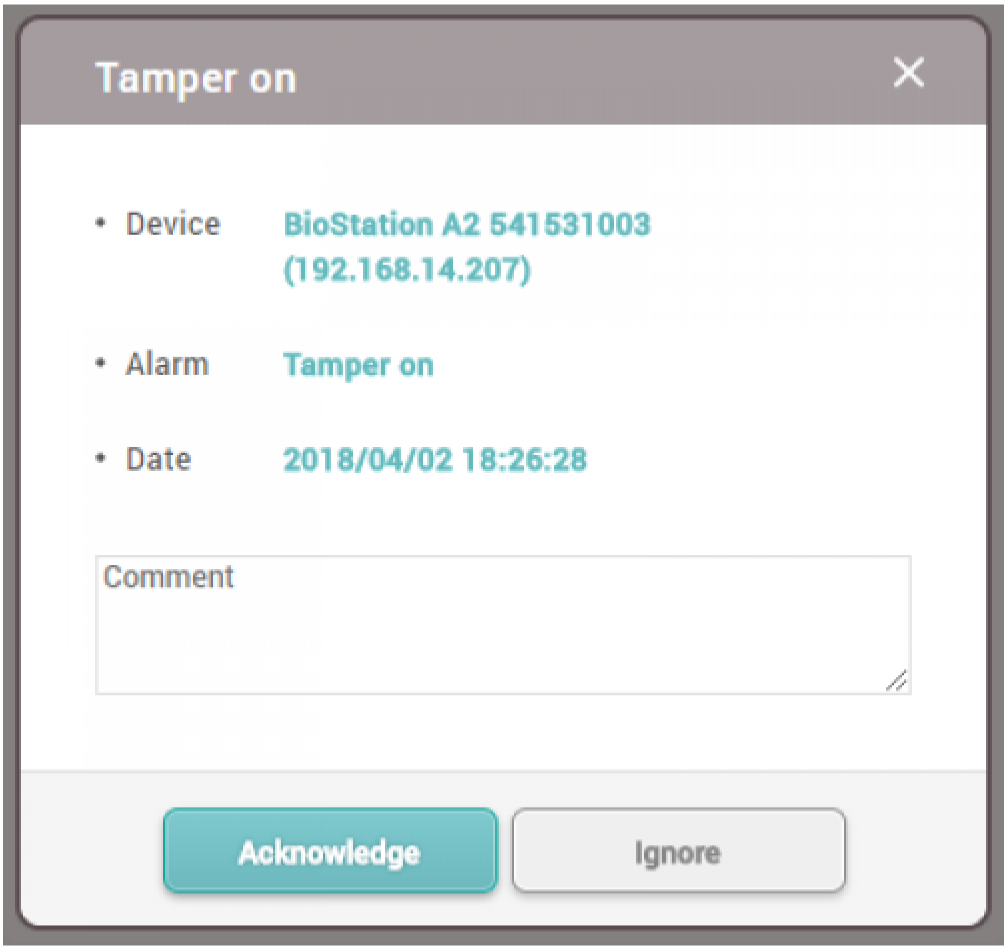
1. Go to Device **Setting** > **Advanced**.
2. Change **Secure Tamper** into **On**.



* Secure Tamper — On

* All the users, logs, and encryption key in the device will be removed at the secure tamper event.

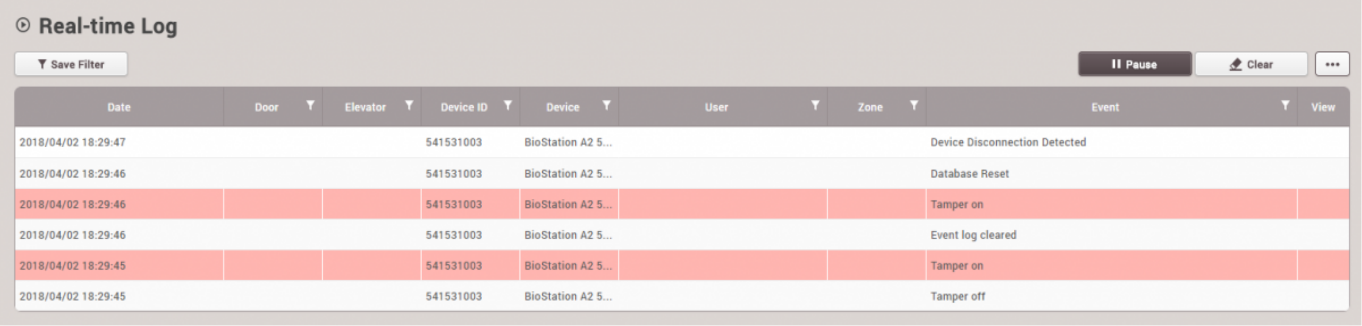
3. When the Tamper On event happens, you can see below message in BioStar 2.



Tamper on

- Device BioStation A2 541531003 (192.168.14.207)
- Alarm Tamper on
- Date 2018/04/02 18:26:28

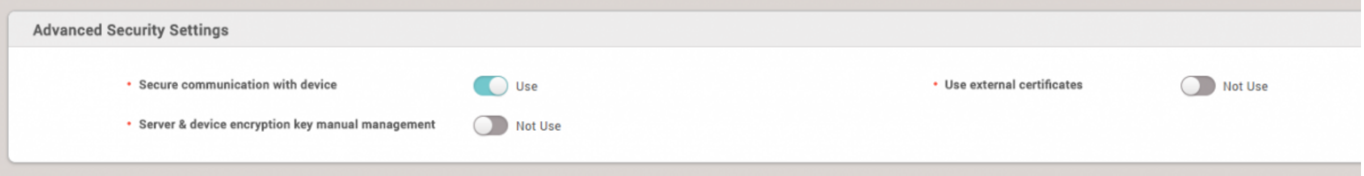
Then, you can see the below event logs in Monitoring section. Especially, if you check the users and logs on the device directly, they would be deleted completely.



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	

Case 2:

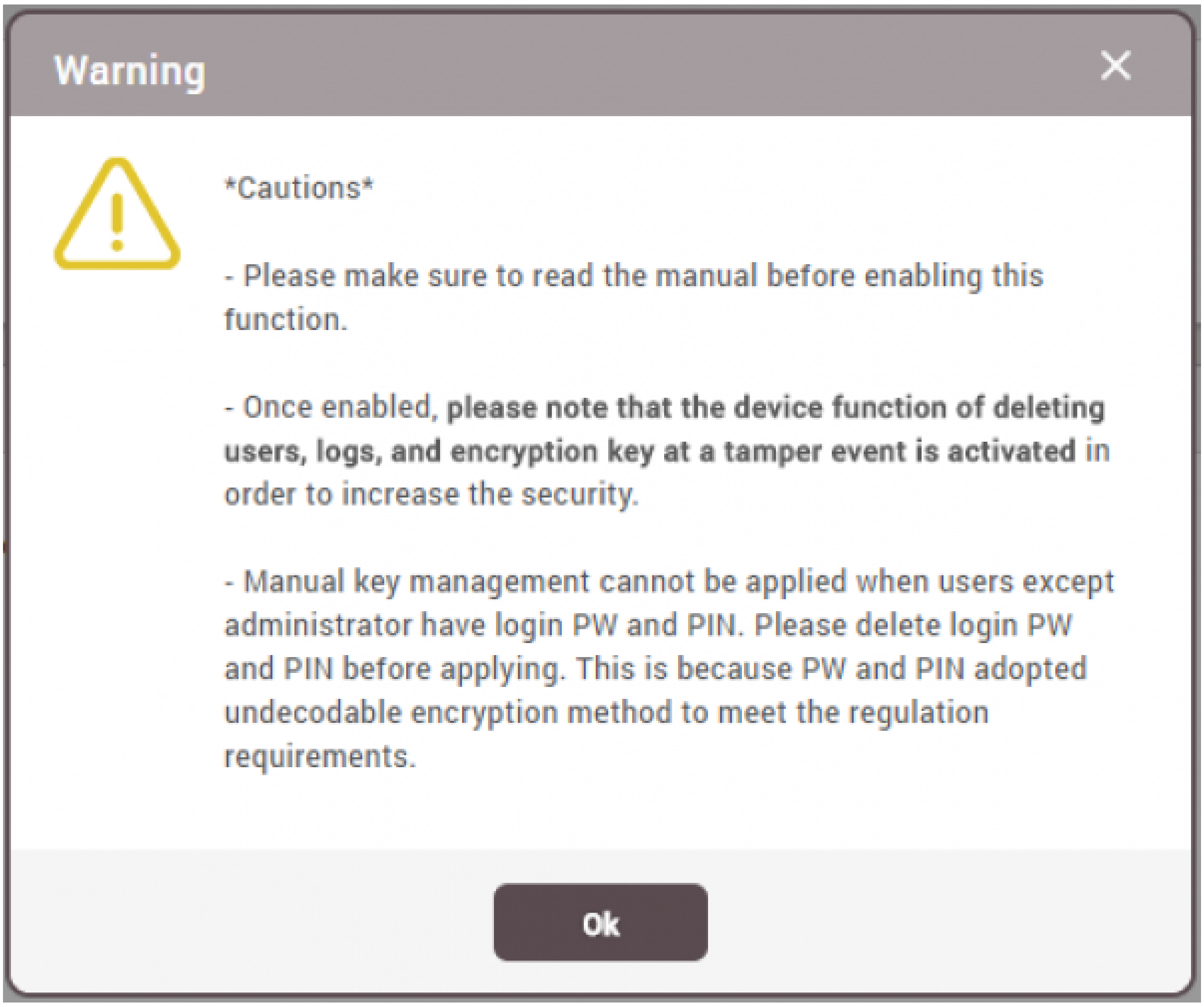
If you set **Secure communication with device** to **Use** in **Setting** > **SERVER**, you can see additional options below. Please see **Server & device encryption key manual management**.



Advanced Security Settings

- Secure communication with device: Use
- Server & device encryption key manual management: Not Use
- Use external certificates: Not Use

If you change **Server & device encryption key manual management** into **Use**, you can see below warning message. Please note that, if you configure this setting, the function **Secure Tamper** will be applied automatically. Before you apply this setting, please be careful.



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.