Table of Contents

How to configure Secure Tamper

When **Tamper On** option is ON: 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:

- BioStation 2 V1.6.0 or above
- BioStation A2 V1.5.0 or above
- BioStation L2 V1.4.0 or above
- CoreStation V1.1.0 or above
- BioEntry P2 V1.1.0 or above
- BioLite N2 V1.0.0 or above
- BioEntry W2 V1.2.0 or above
- BioEntry R2 V1.0.0 or above
- XPass D2 V1.0.0 or above
- FaceStation 2 V1.1.0 or above
- FaceStation F2 V1.0.0 or above
- FaceLite V1.0.0 or above
- X-Station 2 V1.0.0 or above
- BioStation 3 V1.0.0 or above
- BioStation 2a V1.0.0 or above

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

How to configure
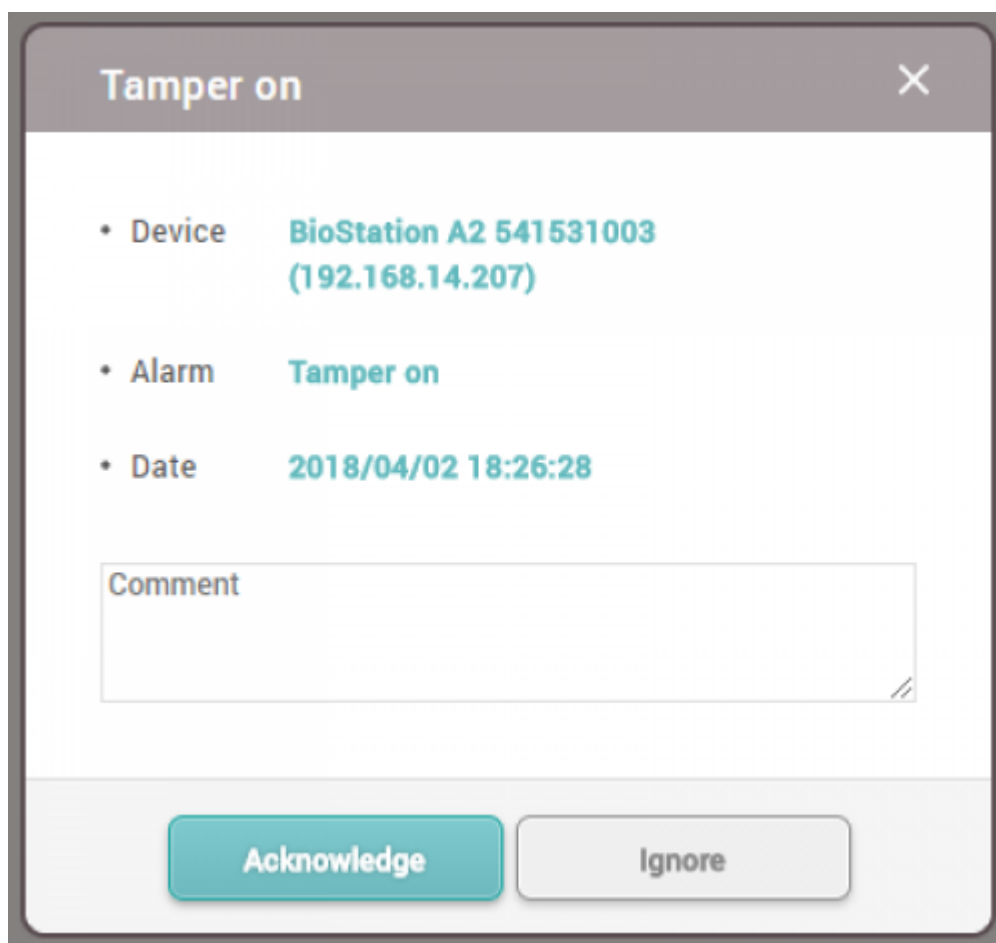
There are two cases to configure.

Case 1:

If you set **Secure communication with device** to **Not Use** in **Setting** > **SERVER**, you should follow below instructions to configure secure tamper.
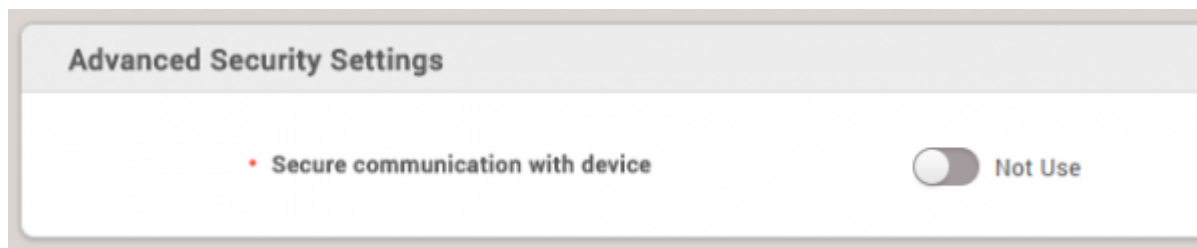
1. Go to Device **Setting** > **Advanced**.
2. Change **Secure Tamper** into **On**.

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

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.

⊙ **Real-time Log**

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	• Use external certificates	⚪ Not Use
• Server & device encryption key manual management	⚪ 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.

From:
https://kb.supremainc.com/knowledge/ -
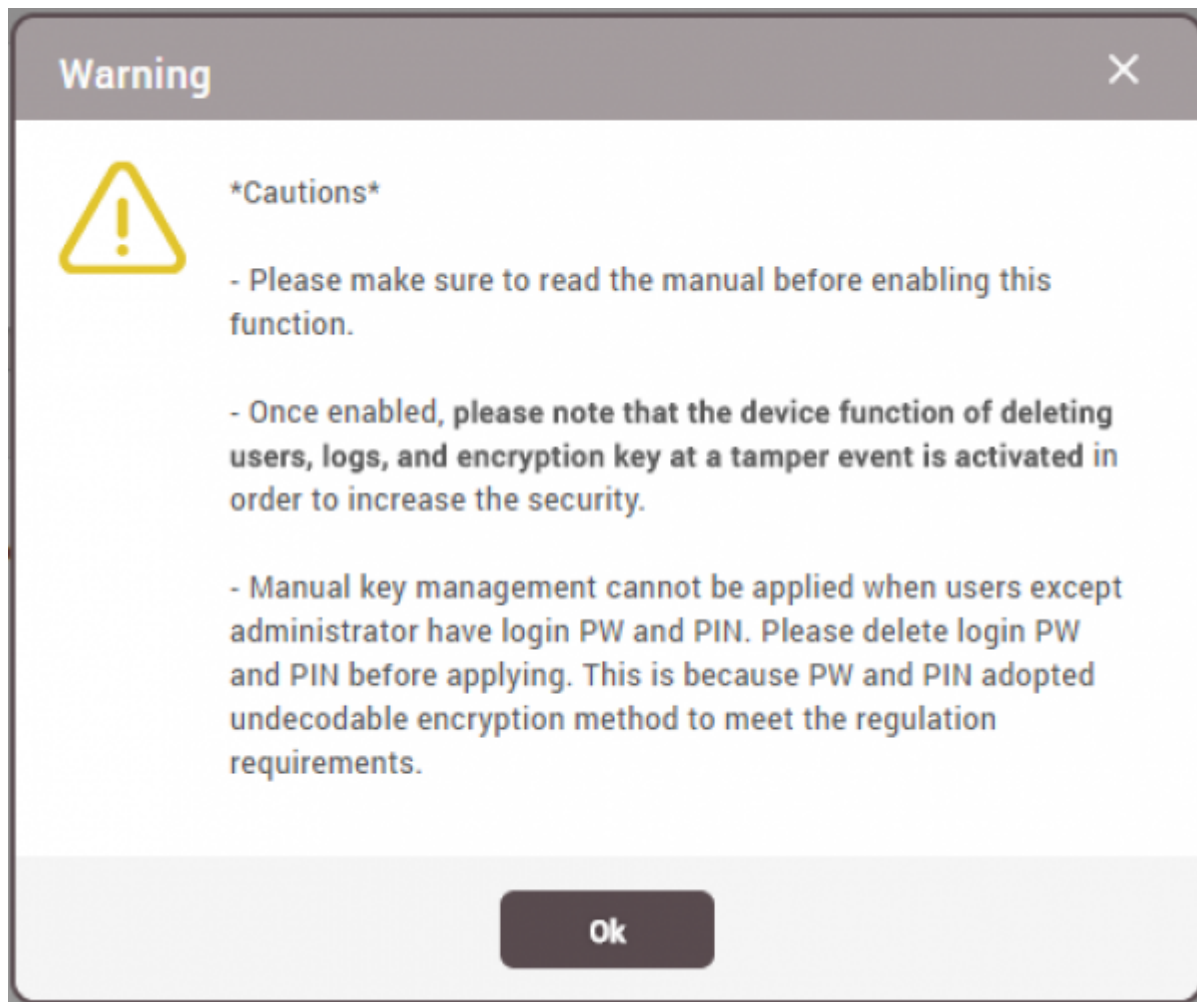
Permanent link:
https://kb.supremainc.com/knowledge/doku.php?id=en:how_to_configure_secure_tamper

Last update: **2024/03/07 08:07**