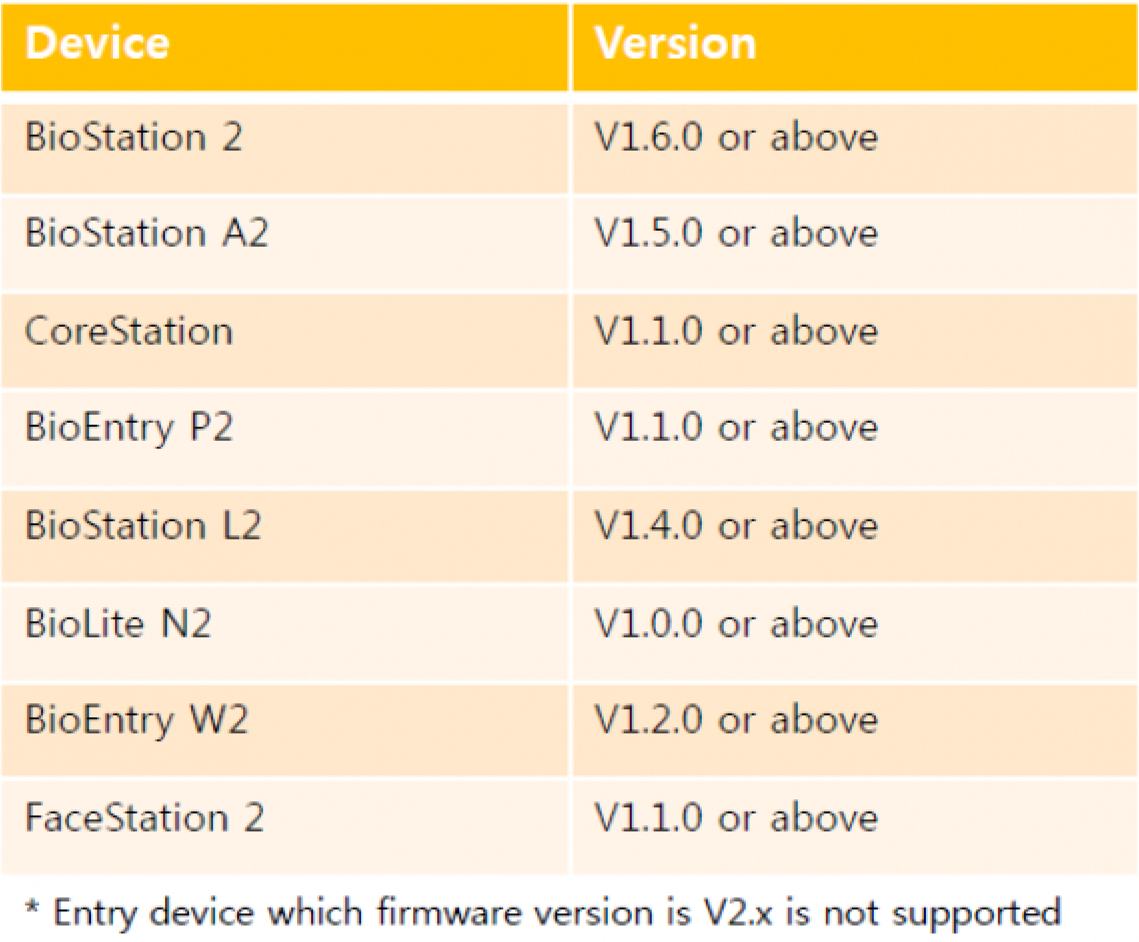
콘텐츠 테이블

- 보안 탬퍼 구성하기 1
  - 구성 방법 2
    - 방법 1: 2
    - 방법 2: 3

보안 탬퍼 구성하기

장치가 브래킷과 물리적으로 분리될 때(**탬퍼 켜짐** 이벤트 발생) 장치에 구성된 모든 사용자, 로그, 암호화 키, SSL 인증서에 대한 데이터가 즉시 삭제됩니다.

지원 장치 및 펌웨어 버전:



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
BioLite 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

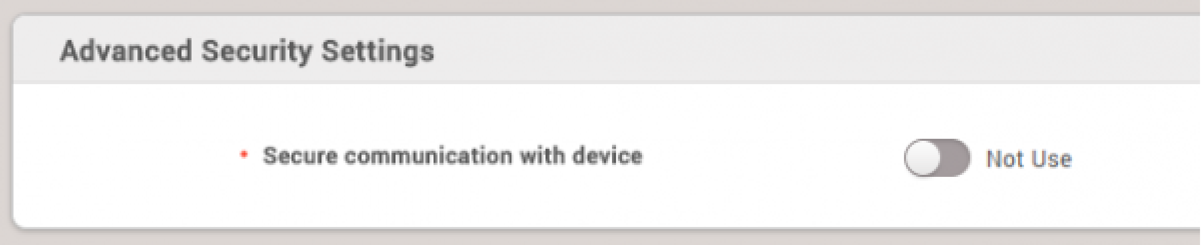
- **탬퍼 켜짐** 이벤트가 발생하면 BioStar 2에 저장된 사용자는 장치와 자동으로 동기화되지 않습니다. 이 경우 사용자를 수동으로 장치로 전송해야 합니다.
- 슬레이브 장치는 지원되지 않습니다.

구성 방법

보안 탬퍼를 구성하는 방법은 두 가지 경우가 있습니다.

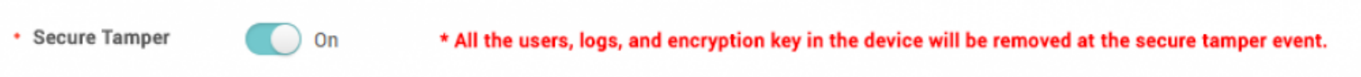
방법 1:

설정(Setting) > **서버(SERVER)**에서 **장치와 보안 통신(Secure communication with device)**을 **사용 안 함(Not Use)**으로 설정한 경우 다음 지침에 따라 보안 탬퍼를 구성해야 합니다.


Advanced Security Settings

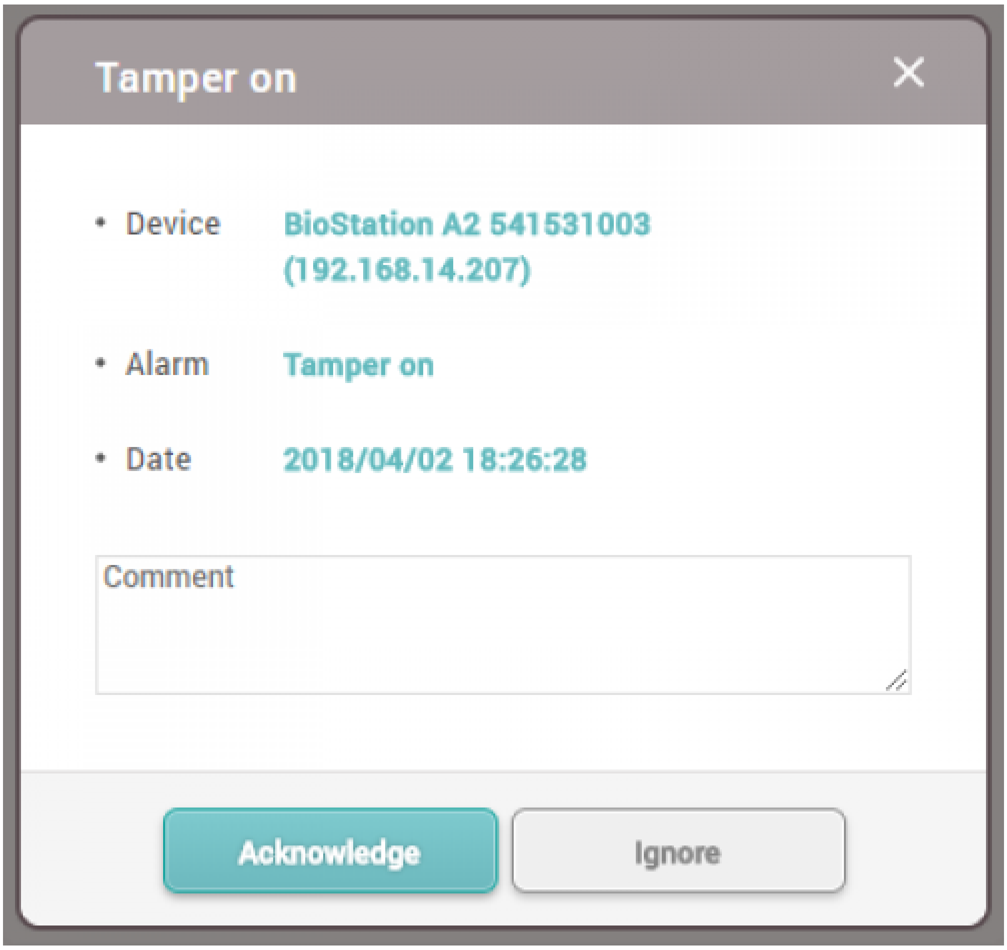
* Secure communication with device Not Use

1. **장치(DEVICE)** 메뉴에서 장치를 선택한 뒤 **고급(Advanced)**을 클릭하십시오.
2. **보안 탬퍼(Secure Tamper)**를 **켬(On)**으로 변경하십시오.


* Secure Tamper On

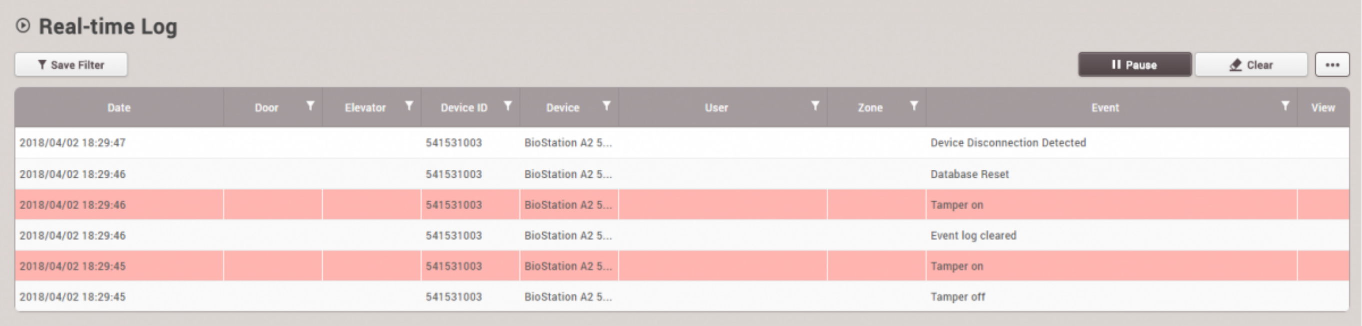
* All the users, logs, and encryption key in the device will be removed at the secure tamper event.

3. **탬퍼 켜짐(Tamper On)** 이벤트가 발생하면 BioStar 2에 다음 메시지가 나타납니다.



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

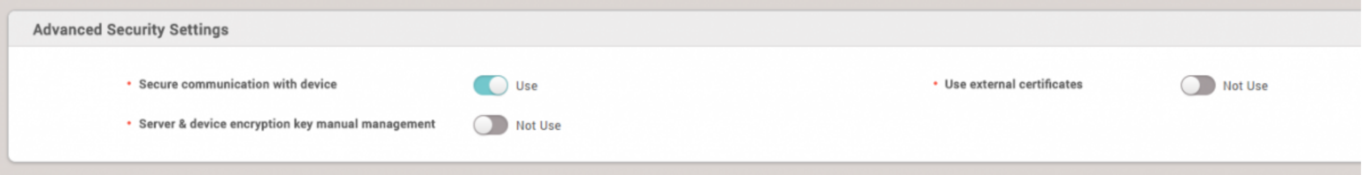
이후 **모니터링** 메뉴에서 다음과 같은 이벤트 로그를 확인할 수 있습니다. 특히 장치의 사용자와 로그를 직접 확인하면 완전히 삭제됩니다.



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	

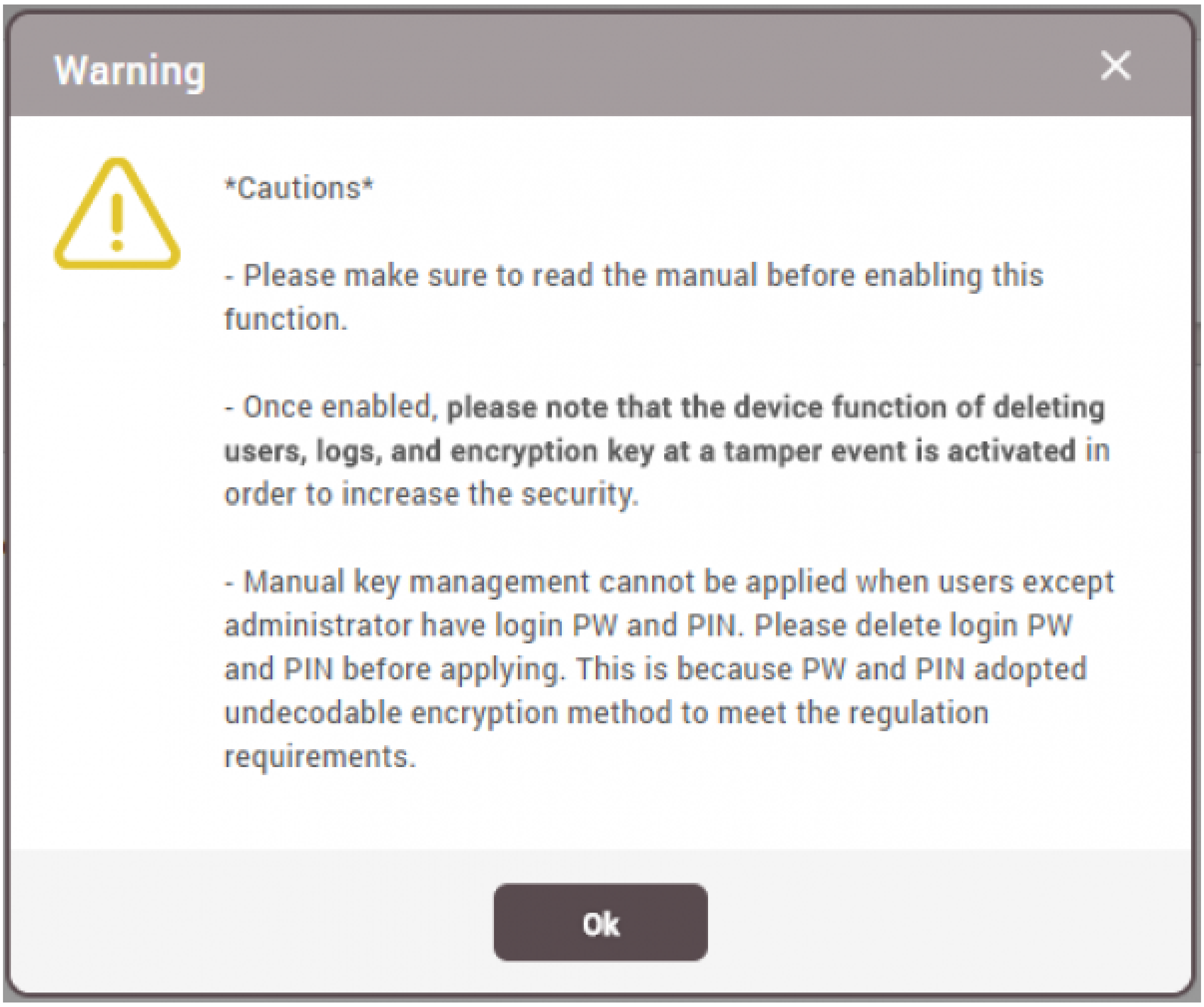
방법 2:

설정(Setting) > **서버(SERVER)**에서 **장치와 보안 통신(Secure communication with device)**을 **사용(Use)**으로 설정하면 추가 옵션을 볼 수 있습니다. **서버 및 장치 암호화 키 수동 관리(Server & device encryption key manual management)**를 확인하십시오.


Advanced Security Settings

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

서버 및 장치 암호화 키 수동 관리(Server & device encryption key manual management)를 **사용(Use)**으로 변경하면 다음과 같은 경고 팝업이 표시됩니다. 이 설정을 구성하면 **보안 탬퍼(Secure Tamper)** 기능이 자동으로 적용됩니다. 이 설정을 적용하기 전 주의하십시오.


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.

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

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

Last update: **2018/07/11 17:14**