

BioStation 2

Firmware Revision Notes

Version 1.8.0

Firmware Version 1.8.0 (Build No. 1.8.0_190806)

Release: 2019-08-08

1. Important Bug Fix

- 1.1. The master device abnormally shuts down if it is operated after reconnecting a disconnected slave device.
- 1.2. Alarms for the held open and forced open are not cleared at the door.
- 1.3. The master device abnormally shuts down if the RS-485 mode of the master device is changed after disconnecting the 31 connected slave devices.

2. New Features and Improvements

2.1. OSDP Standardization

- Improved to comply with OSDP V2.1.7 protocol when connecting with 3rd-party controllers.

2.2. Supports Anti-Tailgating at doors.

2.3. Supports the duplicate fingerprint check when registering users on a device.

2.4. Supports setting options for Wiegand authentication result output.

- User ID and Card ID

2.5. Change the way new settings are applied when adding administrators using batch edit of devices.

- Before: Overwrite a new setting to existing settings.
- After: Add a new setting to existing settings.

2.6. Increase of the number of administrators that can be added.

2.7. Increase of the maximum number of floor levels to up to 2,048.

2.8. Supports options by card type.

2.9. Support to the Clear APB for each user.

2.10. If the data transmission fails when communicating with OSDP, it is transmitted again.

2.11. Support for connecting new devices.

- XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

3. Bug Fix

3.1. Slave device disconnects and alarm cannot be cleared if multiple actions are set for alarms in the global zone.

3.2. The device recognizes the iCLASS Seos card as a CSN card.

3.3. The held open occurs abnormally if the door is configured with a slave device after the slave device reboots.

3.4. Applies FA(False Acceptance) improvement algorithm.

3.5. Start time is not applied in UTC when importing filtered logs using SDK.

3.6. A user cannot access BioStar 1.93 when using the latest firmware.

3.7. Relay works after reconnecting for authentication that occurred when elevator connection is disconnected.

3.8. Access is denied and user ID is displayed abnormally when using a smart card or fingerprint authentication in One Device Mode.

Firmware Version 1.7.1 (Build No. 1.7.1_181204)

Release: 2018-12-11

1. New Features and Improvements
 - 1.1. Improves and adds the features for previous modifications.
 - The bit of the fingerprint image is broken.

Firmware Version 1.7.0 (Build No. 1.7.0_181126)

Release: 2018-11-29

1. Important Bug Fix

- 1.4. Wiegand Out is not output when authenticating with blacklist card.
- 1.5. With Bypass enabled, authentication failure message is not displayed when unregistered ID is authenticated.
- 1.6. The user cannot issue a new File after the App and File are created when issuing the DESFire card.
- 1.7. A code is added to prevent the authentication fails because the cache memory is broken.

2. New Features and Improvements

- 2.1. Support to AES encryption type for DESFire card.
- 2.2. Support to DESFire/DESFire EV1 Advanced option.
- 2.3. Support to the creation of up to 2048 Access Levels and Access Groups.
- 2.4. If a user is registered, modified, or deleted, the event log shows whether the editing was done on the server or on the device.
- 2.5. If the data transmission fails when communicating with OSDP, it is transmitted again.
- 2.6. Improves the data protection.
 - Increase the items to encrypt the data.
 - Support to setting the period for storing the personal information.
 - Support for additional features in Secure Tamper: Delete Users, Logs, Data Encryption Key, SSL certificate, and Smart Card Layout when a secure tamper event occurs.
- 2.7. Change the maximum value of the width for the Wiegand Input.
- 2.8. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
- 2.9. Support for Individual Authentication Successful Messages and Working alarm time reports.
- 2.10. When using The bypass, The card ID is output as Wiegand even though a user authenticates with the AoC.

3. Bug Fix

- 3.1. The alarm can be released in the Floors status after a fire alarm occurs when the elevator is configured as a Fire Alarm Zone.
- 3.2. The relays operate differently from the previous status if the slave device is reconnected.
- 3.3. Modified the firmware of that slave device so that it cannot be upgraded when a device not supported by the master device is connected as a slave.
- 3.4. If a user authenticates the fingerprint consecutively to the slave device, the fingerprint sensor will not operate.
- 3.5. Change some special characters (\, /, :, *, ?, ", ', ` , <, >, |, .) to be unavailable when setting a user name.
- 3.6. An administrator cannot set the permissions of other administrators.
- 3.7. If a user authenticates the card to XPass D2 connected to as a slave device, the beep sounds twice.

- 3.8. 1: N authentication can also be added on the slave device even though the master device is only capable of 1: 1 authentication.
- 3.9. The bit of the fingerprint image is broken.
- 3.10. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
- 3.11. Amharic Unicode characters are not displayed normally.

Firmware Version 1.6.2 (Build No. 1.6.2_180821)

Release: 2018-08-23

1. Bug Fix
 - 1.1. The device restarts when the fingerprint authentication fails.

Firmware Version 1.6.1 (Build No. 1.6.1_180531)

Release: 2018-06-18

1. New Features and Improvements

1.1. Support the bypass mode through Wiegand output on smart cards.

- Bypass mode: It makes the device send out Card Data to 3rd party device without making an authentication. With this mode, the device works as a dummy device, and card data only can be transmitted through Wiegand.

1.2. Support for connecting new devices.

- BioLite N2(BLN2-PAB), XPass D2(XPD2-GDB, XPD2-GKDB)

2. Bug Fix

2.1. Issue where the device restarts when authenticating with an unregistered fingerprint.

Firmware Version 1.6.0 (Build No. 1.6.0_180304)

Release: 2018-03-05

1. New Features and Improvements
 - 1.1. Support Interlock zone, Muster zone.
 - 1.2. Support Daylight Saving Time setting.
 - 1.3. Improves Trigger & Action for duress finger.
 - 1.4. Support Private Authentication on AoC.
 - 1.5. Add and change the function that import & export USB logs and users to be compatible with BioStar 2 V2.6.
 - Before: Provided a folder such as Device Type_Device ID_YYMMDD_HHMM.
 - After: Provides a compressed file such as BioStar2_YYYYMMDD_HHMMSS.tgz.
 - Beginning with V2.6.1 on BioStar 2 platform.
 - 1.6. Improves to handle the encryption key of the important information stored in database differently from server to server.
 - 1.7. Support One Device Mode(Legacy).
 - 1.8. Support simultaneous use of Wiegand input and output.
 - 1.9. Support the secure tamper.
 - 1.10. Support User Photo Display(When authentication is succeed)
 - 1.11. Support connecting with BioLite N2, XPass D2.

Firmware Version 1.5.0 (Build No. 1.5.0_170919)

Release: 2017-09-22

1. New Features and Improvements
 - 1.1. Support the intrusion alarm zone.
 - 1.2. Support the ethernet zone.
 - Ethernet zone: The zone master role is performed by a master device, not the BioStar 2 server, and establishes the zone using Ethernet communication between the devices.
 - 1.3. Support fingerprint enrollment on slave device.
 - 1.4. Improves user transfer speed.
 - 1.5. Support SEOS smart cards (Elite Key).
 - 1.6. Improves performance of SEOS smart card RF reading.
 - 1.7. Performs the Access on Card (AoC) matching when connected to a master device as a slave device.
 - 1.8. Support OP6 sensor.

Firmware Version 1.4.1 (Build No. 1.4.1_170727)

Release: 2017-07-31

1. Bug Fix
 - 1.1. Issue where the device cannot recognize SEOS smart cards when multi-credential authentication mode (iCLASS SEOS card + Fingerprint) is used continuously.

Firmware Version 1.4.1 (Build No. 1.4.1_170707)

Release: 2017-07-31

1. New Features and Improvements
 - 1.1. Support SEOS smart cards.
 - 1.2. Support validation of the device settings.
 - 1.3. User Operator cannot change another user's Operator Level as Administrator.
2. Bug Fix
 - 2.1. Issue where the device is malfunctioned when device log is full.
 - 2.2. Issue where the device is malfunctioned when receiving or sending Wiegand signals.

Firmware Version 1.4.0 (Build No. 1.4.0_170315)

Release: 2017-03-27

1. Bug Fix
 - 1.1. The bootloader and kernel are changed.

Firmware Version 1.4.0 (Build No. 1.4.0_170220)

Release: 2017-02-20

1. New Features and Improvements
 - 1.1. Firmware rebuild due to changing memory capacity.

Firmware Version 1.4.0 (Build No. 1.4.0_170110)

Release: 2017-01-20

1. New Features and Improvements
 - 1.1. Support elevator control.
 - 1.2. Support for alphanumeric ID.
 - 1.3. Support for Secure Communication (SSL & TLS)
 - 1.4. Private authentication mode can be added on access-on-card.
 - 1.5. Up to 100,000 cards can be added to blacklist

Firmware Version 1.3.1 (Build No. 1.3.1_160921)

Release: 2016-09-22

1. Bug Fix
 - 1.1. Memory leak issue when a T&A device is registered as a slave device and users authenticate after pressing a T&A key.
 - 1.2. Issue where the master device reboots when a device with an old firmware version is connected as a slave device and a user authenticates with a card on the slave device.
 - 1.3. Issue where card authentication results did not appear when a slave device is connected.

Firmware Version 1.3.0 (Build No. 1.3.0_160624)

Release: 2016-06-24

1. Added operation condition and action – device sound alarm support
2. NFC support.
3. Support for 256 bit card ID.
4. Support for automatic door configuration.

Firmware Version 1.2.1 (Build No. 1.2.1_160519)

Release: 2016-05-19

1. Bug Fix
 - 1.1. Issue where BS2-OMPW's screen displayed improperly.

Firmware Version 1.2.1 (Build No. 1.2.1_160317)

Release: 2016-03-17

1. Bug Fix
 - 1.1. Logs not transmitting properly when logs in the device reaches the storage limit.

Firmware Version 1.2.0 (Build No. 1.2.0_160204)

Release: 2016-02-04

1. Bug Fix
 - 1.1. Issue with door relay operation.
 - 1.2. Issue where the day only appears in English after changing the theme.
 - 1.3. Issue with alarm lasting time.
 - 1.4. Issue where user ID appears in duplicates.

Firmware Version 1.2.0 (Build No. 1.2.0_160106)

Release: 2016-01-06

1. Support for scheduled lock/unlock zones.
2. Support for global anti-passback.
3. Bug Fix
 - 3.1. Door relay not working properly after restarting the device.

Firmware Version 1.1.0 (Build No. 1.1.0_150908)

Release: 2015-09-08

1. Bug Fix
 - 1.1. Authentication fail issue when authenticating from slave devices.

Firmware Version 1.1.0 (Build No. 1.1.0_150819)

Release: 2015-08-19

1. Bug Fix
 - 1.1. LSB recognition problem with DESFire cards.

Firmware Version 1.1.0 (Build No. 1.1.0_150805)

Release: 2015-08-05

1. Support for DM-20 and third party Wiegand card readers.

Firmware Version 1.0.1 (Build No. 1.0.1_150423)

Release: 2015-04-23

1. Bug Fix
 - 1.1. Fingerprint can't be input when using both anti-passback and dual mode authentication.
 - 1.2. Card information read erroneously when the card's byte order is changed to LSB.

Firmware Version 1.0.0 (Build No. 1.0.0_150312)

Release: 2015-03-12

1. Initial firmware developed.



Suprema Inc.
16F Parkview Tower
248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-863 Republic of Korea
Tel.+82-31-783-4502 Fax.+82-31-783-4503
sales@supremainc.com www.supremainc.com