BioStation 2

Firmware Revision Notes

Version 1.10.1

EN 301.00.BS2 V1.10.1

Firmware Version 1.10.1 (Build No. 1.10.1_211123)

Release: 2022-01-26

1. Bug Fixes
   1.1. When setting the elevator to the scheduled unlock zone and using the 'Started by User Authentication' option, the floor is activated normally when a user belonging to the access group authenticates, but the 'Floor released' logs are output (Affects version: v1.2.0).
   1.2. Improved to check for the duplication of cards registered with users when transmitting user data from the server to devices (Affects version: v1.8.0).
   1.3. If some ports of the OM-120 connected as a slave are set as a door relay and the device is rebooted, the relay was operated abnormally (Affects version: v1.0.0).
   1.4. When loading the logs for the user who entered the admin menu using the SDK, the user ID was not displayed (Affects version: v1.0.0).
   1.5. The device failed to recognize the iCLASS Seos card intermittently before rebooting the device (BS2-OIPW) (Affects version: v1.0.0).
   1.6. The 'Delete the Root Certificate' was not displayed when a user with the administrator level accessed the menu on the device where the certificate was stored (Affects version: v1.9.0).
   1.7. When authenticating on a device that has dual authentication set up, the authentication success sound is not output for the dual authentication result, and the home screen is maintained (Affects version: v1.10.0).
   1.8. Slave devices are disconnected when the master device is rebooted (Affects version: v1.0.0).
   1.9. The user ID was abnormally displayed in the event log if the user authenticated with AoC set as the blacklist card when the User ID Type was set to Alphanumeric (Affects version: v1.0.0).
   1.10. Abnormal authentication failure occurred when the slave device's auth mode was set to card+fingerprint (Affects version: v1.9.0).
   1.11. PIN authentication did not work properly when using Device Hashkey Management (Affects version: v1.9.0).
   1.12. When initializing the master device with the 'Without Network' option, the RS-485 communication key was initialized and the slave device was disconnected (Affects version: v1.0.0).

Firmware Version 1.10.0 (Build No. 1.10.0_210621)

Release: 2021-06-25

1. New Features and Improvements
    1.1. Improved manually turning the secure tamper on or off even when the default hash key is set.
    1.2. Upgraded to the 1.1.1i version of OpenSSL.
    1.3. Separated event logs of Mobile Access cards and RFID cards.

2. Bug Fixes
    2.1. The RS-485 communication did not work properly when connecting the device to a third-party controller via OSDP after activating the Secure Communication mode. (Affects version: v1.9.0 or earlier)
    2.2. The screen was abnormally displayed when the second user authentication was successful on a slave device with dual authentication. (Affects version: v1.10.0 or earlier)
    2.3. After being disconnected from BioStar 2, an incorrect pop-up message was displayed until they were reconnected. (Affects version: v1.9.0 or earlier)
    2.4. The relay operated as Off (Lock) after setting the scheduled unlock zone in the elevator and rebooting the master device. (Affects version: v1.9.0 or earlier)
    2.5. All files in the database were deleted after exporting them to a USB. (Affects version: v1.9.0 or earlier)
    2.6. The slave device rebooted abnormally. (Affects version: v1.9.0 or earlier)
    2.7. Disconnected logs frequently occurred when the device was used with Secure I/O 2. (Affects version: v1.9.0 or earlier)
    2.8. The Wiegand reader operated as Unlock after setting the Wiegand reader connected to DM-20 to Lock and rebooting the device when using the device with DM-20. (Affects version: v1.9.0 or earlier)
    2.9. The door remained locked and did not open after rebooting the device when it was set to Manual Unlock. (Affects version: v1.9.0 or earlier)
    2.10. Ten administrators were still not deleted from the device when initializing the device that has 1,000 assigned administrators. (Affects version: v1.9.0 or earlier)
    2.11. When enrolling a new fingerprint to AoC, it was able to authenticate the user with both the new fingerprint data and the existing fingerprint data. (Affects version: v1.9.0 or earlier)

Firmware Version 1.9.0 (Build No. 1.9.0_200924)

Release: 2020-10-16

1. Important Bug Fix

1.1. Logs generated while the device is disconnected are not sent to BioStar 2, even after the device is reconnected.

1.2. When a user attempted authentication continuously in a short cycle, Wiegand output did not work properly.

2. New Features and Improvements

2.1. Added feature to change device ID.

2.2. Enhancement in the security of the device

- Restrict unencrypted connections.
- Enhancement in security of encryption keys
- Encrypt and migrate user information.

2.3. Improved Anti-passback zone to operate based on the door status.

2.4. Improved the scheduled unlock zone function for each floor when controlling elevator.

2.5. Supports new device.

- XPass D2 (Rev)

2.6. Support to the Mobile Access V1.1.

2.7. Changed the color of LED indicator.

3. Bug Fixes

3.1. An OSDP security session error occurred when connecting the OM-120 and XPass D2 as slave devices.

3.2. If a user set as device administrator was retransmitted, the user could not enter the admin menu.

3.3. When a 'Tamper On' event ouccured after rebooting the master device, only output, of all trigger and actions set in the slave device, was operational.

3.4. When the connection with the master device had been lost due to a secure tamper with the slave device, the device did not connect again.

3.5. When all or user data were exported to a USB and then the user data were imported again after upgrading the device firmware, the event log was deleted.

3.6. An error in the master-slave connection occurred due to the RS-485 communication key.

3.7. When the device was powered off and then on again to update the fingerprint template, the user was deleted.

3.8. When the authentication was being processed on the device after a secure credential card had been issued, an authentication failure occurred with “Auth Unexpected Credential.”

3.9. After a global anti-passback violation, an authentication success log occurred twice.

3.10. An error occurred when authenticating with an iCLASS SEOS card when a smart card layout was set but SEOS was not selected in the card type option.

3.11. PIN authentication failed.

3.12. After upgrading the device firmware, all, user, or log data were not able to be exported to a USB.

3.13. After the message 'Invalid payload' occurred on the slave device, it was disconnected abnormally and reconnection was impossible.

3.14. When a locked device was rebooted for an RS-485 connection, the slave device became unlocked.

3.15. When Factory Default was performed using SDK, the device resource (logo image) did not initialize.

3.16. Authentication of fingerprints registered as duress fingerprints failed.

3.17. Device reboots or a timeout occurred when upgrading firmware or transferring user data during SSL secure communication.

3.18. It was unable to edit, delete or add an authentication mode.

3.19. When the delay for the output signal occurred repeatedly, the device did not work properly.

3.20. When the device was connected as a slave, the output port could not be set in the Trigger and Action.

3.21. Runtime crashed intermittently after initializing the fingerprint sensor.

3.22. When a user authenticated on the slave device using a smart card or the face, the master device would reboot.

3.23. When a user authenticated the fingerprint after setting the byte order as LSB and the Wiegand output information as the user ID, the device would reboot.

3.24. Once a card had been registered on the Wiegand output device, the device would not work properly when trying to output data using a fingerprint registered to another user.

3.25. When the code for generating protocol packets in RFCore-HID SAM exceeded 127, the device did not work properly.

3.26. When the master device wss rebooted with both the scheduled unlock and manual lock set, it operated using the scheduled unlock.

3.27. Slave device with stored certificates failed to connect to the server while using Secure communication with a device.

Firmware Version 1.8.0 (Build No. 1.8.0_190806)

Release: 2019-08-08

1. Important Bug Fix

   1.3. The master device abnormally shuts down if it is operated after reconnecting a disconnected slave device.

   1.4. Alarms for the held open and forced open are not cleared at the door.

   1.5. 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

1.6. Wiegand Out is not output when authenticating with blacklist card.

1.7. With Bypass enabled, authentication failure message is not displayed when unregistered ID is authenticated.

1.8. The user cannot issue a new File after the App and File are created when issuing the DESFire card.

1.9. 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
   1.10. 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
SECURITY & BIOMETRICS

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