BioEntry W2

Firmware Revision Notes

Version 1.4.1

suprema
BIOMETRICS & SECURITY

Firmware Version 1.4.1 (Build No. 1.4.1_190911)

Release: 2019-09-18

1. Bug Fix
   1.1. After a user scans and registers a card on a device set as Wiegand Out device, if an existing user authenticates with a credential other than the card, the Wiegand output will behave abnormally.
   1.2. The device restarts if a user authenticates a fingerprint on the device set as below.
      - Byte Order: LSB
      - Wiegand Out: User ID
   1.3. When using firmware V1.4.0 the connection to the I/O device that using the firmware version below is lost.
      - DM-20 FW V1.1.2
      - OM-120 FW V1.0.0
      - Secure I/O 2 FW V1.2.1
   1.4. The master device intermittently reboots when upgrading the firmware of the slave device.

Firmware Version 1.4.0 (Build No. 1.4.0_190708)

Release: 2019-07-12

1. Important Bug Fix

    1.1. When a door configured in a Scheduled Unlock Zone is opened by a Scheduled Unlock, the door is not locked if the zone is deleted.

    1.2. A code is added to prevent the authentication fails because the cache memory is broken.

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.

    2.3. Supports setting options for Wiegand authentication result output.

    - User ID and Card ID

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

    - Existing: Overwrite a new setting to existing settings.
    - Update: Add a new setting to existing settings.

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

    2.6. Increase of the maximum number of floor levels.

    2.7. Supports options for selection by card type.

    2.8. Support to the Clear APB for each user.

    2.9. Supports checking module firmware version.

    2.10. Supports the latest version of I/O module Micom (V1.3.1).

    2.11. Support for connecting new devices.

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

3. Bug Fix

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

    3.2. The output such as LED status indicator or buzzer is not supported for authentication failure due to Live Finger Detection (LFD).

    3.3. It does not respond to inputs from the slave device when booting the master device.

    3.4. Applies FA 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. The device cannot recognize iCLASS cards issued by the first generation device.

    3.8. Supports unsupported devices (FaceStation 2, FaceLite).

    3.9. HID Prox cards are continously recognized.

3.10. The title of the credential input screen is displayed differently on the master device and the slave device when using multiple authentication mode.
   - Existing: master device (user ID, user name), slave device (user ID)
   - Update: master device and slave device (user ID, user name)

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

Firmware Version 1.3.1 (Build No. 1.3.1_190228)

Release: 2019-03-12

1. Bug Fix
   1.1. The device intermittently recognizes the HID Prox card as an EM card.

Firmware Version 1.3.0 (Build No. 1.3.0_181115)

Release: 2018-11-29

1. Important Bug Fix

   1.1. A code is added to prevent the authentication fails because the cache memory is broken.
   1.2. The device reboots when authenticating with the dual authentication.

2. New Features and Improvements

   2.1. Improves the data protection.
   - Increase the items to encrypt the data.
   - Support to setting the period for storing the personal information.

   2.2. Change the maximum value of the interval and width for the Wiegand Input.
   2.3. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
   2.4. If the data transmission fails when communicating with OSDP, it is transmitted again.
   2.5. The site key is initialized if a secure tamper event occurs.
   2.6. If an administrator has registered, modified, or deleted a user, the event log shows whether the editing was done on the server or on the device.
   2.7. Support to the creation of up to 2048 Access Levels and Access Groups.
   2.8. Support to DESFire/DESFire V1 Advanced option.
   2.9. Support to AES encryption type for DESFire card.
   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. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
   3.2. When communicating with OSDP, the LED color is displayed differently from the setting.
   3.3. The device cannot read CSN because the card recognized as an NFC tag.
   3.4. 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.
   3.5. If the elevator is configured by connecting the OM-120 to the device, the relays operate differently from the previous status when the slave device is rebooted.
   3.6. The alarm can be released in the Floors status after a fire alarm occurs when the elevator is configured as a Fire Alarm Zone.

Firmware Version 1.2.3 (Build No. 1.2.3_180907)

Release: 2018-09-20

1. New Features and Improvements
   1.1. Enhance the solution for the relay processing and restoration.

2. Bug Fix
   2.1. The device does not recognize the iCLASS card intermittently.
   2.2. Modified to exclude an incorrect input when the noise generated in the Wiegand input.

Firmware Version 1.2.2 (Build No. 1.2.2_180710)

Release: 2018-07-24

1. Bug Fix
   1.1. The device restarts when authentication fails.
   1.2. Modified to limit kernel downgrade based on the hardware version of the device.

Firmware Version 1.2.1 (Build No. 1.2.1_180523)

Release: 2018-06-20

1. New Features and Improvements
   1.1. In a device with an LCD, the user name is displayed on the LCD when authentication is successful even when connected in slave mode.
   1.2. Support for connecting new devices.
      - BioLite N2(BLN2-PAB), XPass D2(XPD2-GDB, XPD2-GKDB)

2. Bug Fix
   2.1. Problem that is affected by the schedule set on the device, even though the smart card is set to the bypass card.
   2.2. Issue where the bypass does not work when authentication with AoC in Wiegand output.
   2.3. Issue where event logs and real-time logs are not uploaded normally to BioStar 2.
   2.4. Problem that relay state is not maintained when reconnecting a device connected by RS-485.
   2.5. Issue in which the door relay status operates as On when the device is reconnected after starting and ending the Schedule Unlock with the door relay device disconnected.
   2.6. Problem that the time zone is not initialized even if the factory reset is performed while secure communication and data encryption key are in use.
   2.7. Issue where if the authentication is successful when the device set as door relay is disconnected, the relay will operate according to previous value after reconnection of the device.
   2.8. Problem that does not respond to the input ground.
   2.9. Modified to limit kernel downgrade based on the hardware version of the device.
   2.10. Issue where the device restarts when authenticating with an unregistered fingerprint.

Firmware Version 1.2.0 (Build No. 1.2.0_180317)

Release: 2018-03-26

1. New Features and Improvements
   1.1. Output signal setting for Wiegand reader control.
   1.2. Improves that invalid values can not be entered in the authentication mode, AuthTimeout, MsgTimeout, ScanTimeout, and MatchingTimeout.
   1.3. Support fingerprint enrollment on slave device.
   1.4. Support the intrusion alarm zone, Muster zone and 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.
   1.5. Performs the Access on Card (AoC) matching when connected to a master device as a slave device.
   1.6. Support SEOS smart cards (Elite Key).
   1.7. Improves performance of SEOS smart card RF reading.
   1.8. Improves user transfer speed.
   1.9. Improves log search within device.
   1.10. User Operator cannot change another user's Operator Level as Administrator.
   1.11. Support Reset without Network Settings.
   1.12. Support Daylight Saving Time setting.
   1.13. Improves Trigger & Action for duress finger.
   1.14. Support Private Authentication on AoC.
   1.15. Improves to handle the encryption key of the important information stored in database differently from server to server.
   1.16. Support One Device Mode(Legacy).
   1.17. Added a message asking whether to delete the fingerprint in the database after completing AoC issuance.
   1.18. Support the secure tamper.
   1.19. Support ISO14443A 10 Byte CSN.
   1.20. Support connecting with BioEntry R2, BioEntry P2, BioLite N2, XPass D2.

2. Bug Fix
   2.1. Problem trying to forward commands related to Config during connection after searching RS-485 slave device.
   2.2. Problem not working in 256 bit Wiegand format.
   2.3. Problem with reading mobile smart cards on Galaxy S4.
   2.4. Galaxy S5 NFC is recognized as a CSN card when authenticating with NFC and the authentication fails.
   2.5. Issue where the device can not read HID Prox II card.
   2.6. Issue where the fingerprint sensor does not work.

2.7. Fixed that Hard APB authentication failure notification is distinguished from general authentication failure notification.

2.8. Problem that the user ID type in the slave device can not be set in alphanumeric characters.

2.9. Issue that does not work when template size is set to 384 bytes when issuing NFC card.

2.10. iCLASS 2K card can not be issued as a smart card.

Firmware Version 1.1.5 (Build No. 1.1.5_171026)

Release: 2017-10-30

1. New Features and Improvements
   1.1. Improves Live Finger Detection (LFD) algorithm and changes the calibration method for HW V1.2.0.

Firmware Version 1.1.4 (Build No. 1.1.4_170830)

Release: 2017-09-06

1. New Features and Improvements
   1.1. Improved Live Finger Detection(LFD) performance

2. Bug Fix
   2.1. Issue where the device is reset when the fingerprint is authenticated.

Firmware Version 1.1.3 (Build No. 1.1.3_170717)

Release: 2017-08-07

1. New Features and Improvements
   1.1. Support 8GB eMMC.
   1.2. Performs the validation when invalid values are sent to the device.
   1.3. Support SEOS smart cards.

2. Bug Fix
   2.1. Issue where the device sends an abnormal amount of logs to BioStar.

Firmware Version 1.1.2 (Build No. 1.1.2_170213)

Release: 2017-02-27

1. New Features and Improvements
   1.1. Add Lift I/O MFG Command

2. Bug Fix
   2.1. Issue where the slave device's time zone is changes when the device synchronization is perfomed.
   2.2. Wiegand Output malfunctions when fingerprint authentication is completed after authenticating with the unregistered card
   2.3. Slow-downs the performance.

Firmware Version 1.1.1 (Build No. 1.1.1_161213)

Release: 2016-12-20

1. Bug Fix
    1.1. Issue that cannot detect the device with UDP in BioStar 1.92.

Firmware Version 1.1.0 (Build No. 1.1.0_161201)

Release: 2016-12-13

1. New Features and Improvements
   1.1. Support for the secure communication (TLS) with BioStar 2
   1.2. Support for iCLASS SEOS card
   1.3. Support for the 1.x Template on Card
   1.4. Support for the daylight saving time
   1.5. OP6 sensor support
   1.6. Improved fingerprint algorithm
   1.7. Improved LFD calibration
   1.8. Support for alphanumeric ID
   1.9. Improved RF card specification for BEW2-OHP
      - Before: HID Prox
      - After: HID Prox, EM, MIFARE

Firmware Version 1.0.1 (Build No. 1.0.1_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.

Firmware Version 1.0.0 (Build No.1.0.0_160531)

Release: 2016-05-31

1. Initial firmware developed.

suprema
BIOMETRICS & SECURITY

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