BioEntry P2

Firmware Revision Notes

Version 1.4.1

Firmware Version 1.4.1 (Build No. 1.4.1_210511)

Release: 2021-06-01

1. New features and improvements
   1.1. Upgraded to the 1.1.1i version of OpenSSL.
   1.2. Intelligent Slave Support
      - Intelligent Slave: A function that enables 1:1 or 1:N matching directly from the Suprema device and transmits the authentication result as OSDP card data to the third-party controller.
   1.3. Separated event logs of Mobile Access cards and RFID cards.

2. Bug Fix
   2.1. When calling the BS2_ResetConfigExceptNetInfo API from the BioStar 2 Device SDK, a 'Timeout' error occurred. (Affects version: v1.0.0)
   2.2. Card data were output with the wrong BitCount while the device was communicating with a 3rd party controller via OSDP. (Affects version: v1.0.0)
   2.3. When using a static IP while DNS server address was configured, a reboot on the device caused communication problems between the server. (Affects version: v1.0.0)
   2.4. While the device was communicating with a 3rd party controller via OSDP, the device connected as a slave responded that it supported transparent mode by OSDP_PDCAP even though it did not actually support that mode. (Affects version: v1.0.0)
   2.5. If 31 slave devices were connected and one of the devices got disconnected, the master device rebooted. (Affects version: v1.0.0)
   2.6. Fingerprint authentication did not work after downgrading from firmware version 1.4.0 to firmware version 1.2.1. (Affects version: v1.4.0)
   2.7. It was not able to communicate with a 3rd-party controller via OSDP with the default key before network initialization. (only for devices released with the firmware version 1.4.0 or later) (Affects version: v1.4.0)
   2.8. It was able to communicate using default keys after changing the key settings when the device was connected to a 3rd-party device via OSDP. (Affects version: v1.3.0)
   2.9. After initializing the slave device's settings, it was not able to connect it to a 3rd-party controller. (Affects version: v1.0.0)
   2.10. Secure communication was not available by using the default key after downgrading firmware to version 1.3.1 or below which does not support encryption. (Affects version: v1.4.0)

Firmware Version 1.4.0 (Build No. 1.4.0_200625)

Release: 2020-07-13

1. New features and improvements
   1.1. Added feature to change device ID.
   1.2. Enhancement in the security of the device.
      - Restrict unencrypted connections.
      - Enhancement in the security of encryption keys.
      - Encrypt and migrate user information.
   1.3. Improved Anti-passback zone to operate based on the door status.
   1.4. Improved the scheduled unlock zone function for each floor when controlling elevator.
   1.5. Supports new device.
      - XPass D2 (Rev 2)
   1.6. Changed the color of LED indicator.

2. Bug Fix
   2.1. OSDP Communication does not work normally if the value sent to the slave device is greater than the defined value.
   2.2. The event log of the device is not sent in the order in which it occurred.
   2.3. Issue that the option for card types is deactivated when the device is connected as a slave after the factory reset.
   2.4. Issue that the connection of the slave device is disconnected when the slave device is connected.
   2.5. Improved the device to recognize unknown cards by selecting the card type options. (BEP2-OA)
   2.6. The device reboots or a timeout occurs when upgrading firmware or transferring user data during SSL secure communication.

Firmware Version 1.3.1 (Build No. 1.3.1_190911)

Release: 2019-09-19

1. New features and improvements
    1.1. Improved the speed at which the device recognizes 13.56 MHz cards.

2. Bug Fix
    2.1. The device recognizes the DESFire(Adv) card as a CSN if the device is restarted when the smart card layout set as DESFire(Adv).
    2.2. When using firmware V1.3.0 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
    2.3. The device restarts if a user authenticates a fingerprint on the device set as below.
        - Byte Order: LSB
        - Wiegand Out: User ID
    2.4. 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.
    2.5. The master device intermittently reboots when upgrading the firmware of the slave device.

Firmware Version 1.3.0 (Build No. 1.3.0_190626)

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

   2.5. Increase of the maximum number of floor levels.

   2.6. Supports options for selection by card type.

   2.7. Support to the Clear APB for each user.

   2.8. Supports checking module firmware version.

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

   2.10. Firmware upgrade status is added to LED status indicator.

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

   3.3. Applies FA improvement algorithm.

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

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

   3.6. The device cannot recognize iCLASS cards issued by the first generation device.

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

   3.8. HID Prox cards are continously recognized.

   3.9. 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)

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

Firmware Version 1.2.1 (Build No. 1.2.1_190304)

Release: 2019-03-12

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

Firmware Version 1.2.0 (Build No. 1.2.0_181119)

Release: 2018-11-29

1. Important Bug Fix

1.1. When using iCLASS Seos card, the card does not work as set even though the key setting is changed.

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

2. New features and improvements

2.1. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.

2.2. Change the maximum value of the interval and width for the Wiegand Input.

2.3. Improves the data protection.

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

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 AES encryption type for DESFire card.

2.9. Support to DESFire/DESFire EV1 Advanced option.

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 1.1.2 (Build No. 1.1.2_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 1.1.1 (Build No. 1.1.1_180720)

Release: 2018-07-25

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.
        - XPass D2(XPD2-GDB, XPD2-GKDB)

2. Bug Fix
    2.1. The bypass does not work when authentication with AoC in Wiegand output.
    2.2. Event logs and real-time logs are not uploaded normally to BioStar 2.
    2.3. The relay state is not maintained when reconnecting a device connected by RS-485.
    2.4. The time zone is not initialized even if the factory reset is performed while secure communication and data encryption key are in use.
    2.5. The relay operates according to previous value after reconnection of the device if the authentication is successful when the device set as door relay is disconnected.
    2.6. The device restarts when authentication fails.
    2.7. The RF module of the device gets damaged when using a 13.56 MHz card.

Firmware Version 1.1.0 (Build No. 1.1.0_180317)

Release: 2018-03-26

1. New Features and Improvements
    1.1. Support Muster zone.
    1.2. Support Reset without Network Settings.
    1.3. Support Daylight Saving Time setting.
    1.4. Improves Trigger & Action for duress finger.
    1.5. Support Private Authentication on AoC.
    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. Added a message asking whether to delete the fingerprint in the database after completing AoC issuance.
    1.9. Support the secure tamper.
    1.10. Support ISO14443A 10 Byte CSN.
    1.11. Support connecting with BioLite N2, XPass D2.

2. Bug Fix
    2.1. iCLASS 2K card can not be issued as a smart card.
    2.2. Problem with reading mobile smart cards on Galaxy S4.
    2.3. Galaxy S5 NFC is recognized as a CSN card when authenticating with NFC and the authentication fails.
    2.4. Issue that does not work when template size is set to 384 bytes when issuing NFC card.
    2.5. Fixed that Hard APB authentication failure notification is distinguished from general authentication failure notification.
    2.6. Issue where the device can not read HID Prox II card.
    2.7. Fixed to generate buzzer or sound when starting the intrusion alarm.
    2.8. Problem that delay time of Action Signal Output is not applied in the slave device.
    2.9. Fixed to the device operates in the input waiting state until the authentication time is exceeded when a Wiegand card that is different from the Wiegand format set in the device is input after Arm / Disarm card input.
    2.10. Problem where the response rate was slow when Arm / Disarm occurred.
    2.11. Fixed to Entrance Limit Soft log to be recorded when authentication exceeds the allowed number.

Firmware Version 1.0.0 (Build No.1.0.0_170904)

Release: 2017-09-04

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