BioEntry P2

Firmware Revision Notes

Version 1.5.2

English

EN 301.00.BEP2

suprema

SECURITY & BIOMETRICS

Firmware Version 1.5.2 (Build No. 1.5.2_240508)

Release: 2024-05-09

- BEP2-OA type of BioEntry P2 model support HID iCLASS card type through SE processor.
  For devices with the new SE processor, after upgrading the firmware to v1.4.4 or later, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version. Devices with existing SE processor can be downgraded to a lower version.
- Devices with the software based **Live Finger Detection** cannot downgrade to a lower version after upgrading the firmware to v1.5.1 or later.
- For more information, check the serial number of the device and contact the Suprema. (supremainc.com)

New Features and Improvements

1. Improved to get user update succeeded event log using the GetLogWithFilter function in the SDK.
2. Supports new device.
   - BioStation 2a (BS2A-ODPB, BS2A-OAPWB)
3. Improved to allow the use of **Secure Tamper** regardless of the **Device Hashkey Management** option.

Bug Fixes

1. When authenticating an iClass AoC card and a fingerprint simultaneously, the device restarts abnormally. (Affects version: v1.0.0)
2. The user ID stored as a 32-character string is truncated to only 31 characters in a specific event log. (Affects version: v1.0.0)
3. When a user with a 32-character user ID authenticates to the device while the device is not connected to the server, the authentication event log is not updated in BioStar 2 even after the device is reconnected to the server. (Affects version: v1.0.0)
4. After a firmware upgrade, authentication failure occurs with the previously used cards. (Affects version: v1.5.1)
5. Disabling the **Time Synchronization with Server** setting on the device details page in BioStar 2, then getting the device time, subsequently changing the device time to a previous time, and clicking **Set Time** results in the device restarting abnormally. (Affects version: v1.5.1)

Firmware Version 1.5.1 (Build No. 1.5.1_231113)

Release: 2023-11-20

- BEP2-OA type of BioEntry P2 model support HID iCLASS card type through SE processor.
  For devices with the new SE processor, after upgrading the firmware to v1.4.4 or later, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version. Devices with existing SE processor can be downgraded to a lower version.
- Devices with the software based **Live Finger Detection** cannot downgrade to a lower version after upgrading the firmware to v1.5.1 or later.
- For more information, check the serial number of the device and contact the Suprema. (supremainc.com)

New Features and Improvements

6. XPass D2 new BLE (Bluetooth Low Energy) chip firmware (Build No. 1.7.0_220921) support.
   - The BLE chip parts of the hardware have been changed, and the firmware has been upgraded to be compatible with both the existing and new BLE chips.
7. Supports **Custom Smart Card Layout**.
8. Separated the log related to the cause of the door unlock.
   - Door open request by exit button.
   - Door open request by operator.
9. Added relay deactivation option for exit button input.
   - Added the option to set the door open request log to occur but the relay not to operate when the exit button is pressed.
10. Added software based **Live Finger Detection**.
11. Improved to select and update only the desired information when updating user information. (Compatible with BioStar v2.9.0 or later)
12. Improved the Arm/Disarm status is maintained if the device loses power.
13. Supports setting the byte order for smart cards.
    - Supports setting the byte order of data to be output to Wiegand or OSDP.
14. Improved synchronization to complete if user enrollment fails when synchronizing multiple users to the device in BioStar 2.

Bug Fixes

1. Device does not recognize some MIFARE Classic cards. (Affects version: v1.0.0)
2. Deleting all users included in an access group in BioStar 2 does not delete the access group from the device's user information. (Affects version: v1.0.0)
3. Device does not recognize certain HID iCLASS Seos cards. (Affects version: v1.0.0)

Firmware Version 1.4.4 (Build No. 1.4.4_220914)

Release: 2022-09-14

- BEP2-OA type of BioEntry P2 model support HID iCLASS card type through SE processor.
  For devices with the new SE processor, after upgrading the firmware to v1.4.4 or later, you cannot downgrade to a lower version and downgrade the firmware customized in the lower version. Devices with existing SE processor can be downgraded to a lower version.
- For more information, check the serial number of the device and contact the Suprema. (supremainc.com)

New Features and Improvements

1. Supports the dual SE processor.

Bug Fixes

1. Incorrect Bit Count and card data were output when the Suprema device was connected to a 3rd-party controller via OSDP and the CSN card was registered in Wiegand format and authenticated. (Affects version: v1.4.3)
2. Device does not recognize some HID iCLASS Seos cards. (Affects version: v1.0.0)
3. Event logs and real-time logs are not output due to corrupted log records. (Affects version: v1.0.0)
4. Improved the structure to prevent authentication fail caused by broken database or cache memory. (Affects version: v1.0.0)

Firmware Version 1.4.3 (Build No. 1.4.3_211213)

Release: 2022-01-25

New Features and Improvements

1. Improved to transmit entire card data, including the parity bit, when a user authenticated the fingerprint while the Wiegand card was registered.

Bug Fixes

1. The card ID was always output as MSB through OSDP when the card ID is input while the device was connected by an intelligent slave. (Affects version: v1.4.1)
2. 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)
3. The device failed to recognize the iCLASS Seos card intermittently before rebooting the device. (BEP2-OA) (Affects version: v1.0.0)
4. When the device is connected as an intelligent slave and the first card registered to the user is a Wiegand card of a format other than 26-bit, the CSN value is output through OSDP when authenticated with the user's fingerprint. (Affects version: v1.4.1)
5. The fingerprint sensor was deactivated after upgrading the firmware to v1.4.2 and it was reactivated only when the device is restarted. (Affects version: v1.4.2)

Firmware Version 1.4.2 (Build No. 1.4.2_211018)

Release: 2021-10-22

Bug Fixes

1. When upgrading firmware from v1.1.0 or earlier to v1.4.1, the device failed and could not be recovered. (Affects version: v1.1.0 or earlier)

Firmware Version 1.4.1 (Build No. 1.4.1_210511)

Release: 2021-06-01

New Features and Improvements

1. Upgraded to the 1.1.1i version of OpenSSL.
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.
3. Separated event logs of Mobile Access cards and RFID cards.

Bug Fixes

1. When calling the BS2_ResetConfigExceptNetInfo API from the BioStar 2 Device SDK, a 'Timeout' error occurred. (Affects version: v1.0.0)
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)
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)
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)
5. If 31 slave devices were connected and one of the devices got disconnected, the master device rebooted. (Affects version: v1.0.0)
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)
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)
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)
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)
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

New Features and Improvements

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

Bug Fixes

1. OSDP Communication does not work normally if the value sent to the slave device is greater than the defined value.
2. The event log of the device is not sent in the order in which it occurred.
3. Issue that the option for card types is deactivated when the device is connected as a slave after the factory reset.
4. Issue that the connection of the slave device is disconnected when the slave device is connected.
5. Improved the device to recognize unknown cards by selecting the card type options. (BEP2-OA)
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

New Features and Improvements

1. Improved the speed at which the device recognizes 13.56 MHz cards.

Bug Fixes

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. 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
3. The device restarts if a user authenticates a fingerprint on the device set as below.
   - Byte Order: LSB
   - Wiegand Out: User ID
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.
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

Main Fixes

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

New Features and Improvements

1. OSDP Standardization
   - Improved to comply with OSDP V2.1.7 protocol when connecting with 3rd-party controllers.
2. Supports Anti-Tailgating.
3. Supports setting options for Wiegand authentication result output.
   - User ID and Card ID
4. Increase of the number of administrators that can be added.
5. Increase of the maximum number of floor levels.
6. Supports options for selection by card type.
7. Support to the Clear APB for each user.
8. Supports checking module firmware version.
9. Supports the latest version of I/O module Micom (V1.3.1).
10. Firmware upgrade status is added to LED status indicator.
11. Support for connecting new devices.
    - XPass 2(XP2-MDPB, XP2-GDPB, XP2-GKDPB)

Bug Fixes

1. The device recognizes the iCLASS Seos card as a CSN card.
2. It does not respond to inputs from the slave device when booting the master device.
3. Applies FA improvement algorithm.
4. Start time is not applied in UTC when importing filtered logs using SDK.
5. A user cannot access BioStar 1.93 when using the latest firmware.
6. The device cannot recognize iCLASS cards issued by the first generation device.
7. Supports unsupported devices. (FaceStation 2, FaceLite)
8. HID Prox cards are continously recognized.
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)
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

Bug Fixes

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

Main Fixes

1. When using iCLASS Seos card, the card does not work as set even though the key setting is changed.
2. A code is added to prevent the authentication fails because the cache memory is broken.

New Features and Improvements

1. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
2. Change the maximum value of the interval and width for the Wiegand Input.
3. Improves the data protection.
   - Increase the items to encrypt the data.
   - Support to setting the period for storing the personal information.
4. If the data transmission fails when communicating with OSDP, it is transmitted again.
5. The site key is initialized if a secure tamper event occurs
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.
7. Support to the creation of up to 2048 Access Levels and Access Groups.
8. Support to AES encryption type for DESFire card.
9. Support to DESFire/DESFire EV1 Advanced option.
10. When using The bypass, The card ID is output as Wiegand even though a user authenticates with the AoC.

Bug Fixes

1. If the user uses the BS_GetLogBlob command to get the door ID, the door ID is not output normally.
2. When communicating with OSDP, the LED color is displayed differently from the setting.
3. The device cannot read CSN because the card recognized as an NFC tag.
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.
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.
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

New Features and Improvements

1. Enhance the solution for the relay processing and restoration.

Bug Fixes

1. The device does not recognize the iCLASS card intermittently.
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

New Features and Improvements

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.
2. Support for connecting new devices.
   - XPass D2(XPD2-GDB, XPD2-GKDB)

Bug Fixes

1. The bypass does not work when authentication with AoC in Wiegand output.
2. Event logs and real-time logs are not uploaded normally to BioStar 2.
3. The relay state is not maintained when reconnecting a device connected by RS-485.
4. The time zone is not initialized even if the factory reset is performed while secure communication and data encryption key are in use.
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.
6. The device restarts when authentication fails.
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

New Features and Improvements

1. Support Muster zone.
2. Support Reset without Network Settings.
3. Support Daylight Saving Time setting.
4. Improves Trigger & Action for duress finger.
5. Support Private Authentication on AoC.
6. Improves to handle the encryption key of the important information stored in database differently from server to server.
7. Support One Device Mode (Legacy).
8. Added a message asking whether to delete the fingerprint in the database after completing AoC issuance.
9. Support the secure tamper.
10. Support ISO14443A 10 Byte CSN.
11. Support connecting with BioLite N2, XPass D2.

Bug Fixes

1. iCLASS 2K card can not be issued as a smart card.
2. Problem with reading mobile smart cards on Galaxy S4.
3. Galaxy S5 NFC is recognized as a CSN card when authenticating with NFC and the authentication fails.
4. Issue that does not work when template size is set to 384 bytes when issuing NFC card.
5. Fixed that Hard APB authentication failure notification is distinguished from general authentication failure notification.
6. Issue where the device can not read HID Prox II card.
7. Fixed to generate buzzer or sound when starting the intrusion alarm.
8. Problem that delay time of Action Signal Output is not applied in the slave device.
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.
10. Problem where the response rate was slow when Arm / Disarm occurred.
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

Initial Firmware Developed.

Suprema Inc.

17F Parkview Tower, 248, Jeongjail-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 13554, Rep. of KOREA

Tel: +82 31 783 4502 | Fax: +82 31 783 4503 | Inquiry: sales_sys@supremainc.com

For more information about Suprema's global branch offices,
visit the webpage below by scanning the QR code.
https://supremainc.com/en/about/global-office.asp