BioEntry W2

RELEASE NOTES

Version 1.8.3

English
EN 301.00.BEW2

suprema
SECURITY & BIOMETRICS

CONTENTS

- Firmware Version 1.8.3
- Firmware Version 1.8.2
- Firmware Version 1.8.1
- Firmware Version 1.8.0
- Firmware Version 1.7.1
- Firmware Version 1.7.0
- Firmware Version 1.6.3
- Firmware Version 1.6.2
- Firmware Version 1.6.1
- Firmware Version 1.6.0
- Firmware Version 1.5.0
- Firmware Version 1.4.1
- Firmware Version 1.4.0
- Firmware Version 1.3.1
- Firmware Version 1.3.0
- Firmware Version 1.2.3
- Firmware Version 1.2.2
- Firmware Version 1.2.1
- Firmware Version 1.2.0
- Firmware Version 1.1.5
- Firmware Version 1.1.4
- Firmware Version 1.1.3

Firmware Version 1.1.2

Firmware Version 1.1.1

Firmware Version 1.1.0

Firmware Version 1.0.1

Firmware Version 1.0.0

Firmware Version 1.8.3 (Build No. 1.8.3_260807)

Release | 2026-08-25

Caution

Devices with the new SE processor cannot downgrade to a lower version after upgrading the firmware to v1.7.1 or later. 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.

New Features and Improvements

1. Improved BLE stability.

Bug Fixes

1. Suprema Mobile Access authentication failing on certain Android devices. Affects version: 1.0.0

Firmware Version 1.8.2 (Build No. 1.8.2_241025)

Release | 2024-11-01

> **Caution**
> Devices with the new SE processor cannot downgrade to a lower version after upgrading the firmware to v1.7.1 or later. 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.

New Features and Improvements

1. Improved to not recognize SEOS configuration cards as CSN for 1 minute after device booting.

Bug Fixes

1. When the device is restarted with the **Primary Key** set only in the **Suprema Smart Card Layout** and the **Secondary Key** set only in the **Custom Smart Card Layout**, the device recognizes the Custom Smart Card as a CSN card. Affects version: 1.8.0
2. Some devices fail to boot after a firmware upgrade. Affects version: 1.5.0
3. Some cards are recognized differently from the settings in the **Suprema Smart Card** option. Affects version: 1.4.1
4. **Custom Smart Card Layout** set through **Batch Edit** is not applied on the device detail page. Affects version: 1.8.0
5. When the device log is full and a new event occurs, unintended logs are retrieved with the newly generated event. Affects version: 1.7.0
6. When the **Time Synchronization with Server** option is disabled and the device time is changed, the device restarts abnormally. Affects version: 1.0.0
7. Some smart cards fail to be recognized in environments using the new SE chip firmware. Affects version: 1.7.1
8. DESFire smart cards with the **Custom Smart Card Layout** set to **Secondary Key** are recognized as CSN cards. Affects version: 1.8.0
9. **Custom Smart Card** option does not appear on the device detail page when **RS-485** mode is set to **Slave**. Affects version: 1.8.0
10. Custom smart cards with the **DESFire Advanced** option enabled fail to be recognized. Affects version: 1.8.0

Firmware Version 1.8.1 (Build No. 1.8.1_240508)

Release | 2024-05-09

> **Caution**
> Devices with the new SE processor cannot downgrade to a lower version after upgrading the firmware to v1.7.1 or later. 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.

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: 1.0.0
2. The user ID stored as a 32-character string is truncated to only 31 characters in a specific event log.
   Affects version: 1.0.0
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: 1.0.0
4. After a firmware upgrade, authentication failure occurs with the previously used cards. Affects version: 1.8.0

Firmware Version 1.8.0 (Build No. 1.8.0_231023)

Release | 2023-10-23

> **Caution**
> Devices with the new SE processor cannot downgrade to a lower version after upgrading the firmware to v1.7.1 or later. 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.

New Features and Improvements

1. 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.
2. Supports **Custom Smart Card Layout**.
3. Added software based **Live Finger Detection**.
4. Improved to select and update only the desired information when updating user information. (Compatible with BioStar v2.9.0 or later)
5. Improved synchronization to complete if user enrollment fails when synchronizing multiple users to the device in BioStar 2.
6. Improved smartcard output byte order setting.
    - When using Wiegand or OSDP output, it is improved to be affected by the smartcard output byte order when the Wiegand output information is set to send user ID.

Bug Fixes

1. When authenticating with a BLE mobile card running on iOS, authentication fails and the device restarts intermittently. Affects version: 1.0.0
2. Device does not recognize certain MIFARE Classic cards. Affects version: 1.0.0
3. 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: 1.0.0
4. Device does not recognize certain HID iCLASS Seos cards. Affects version: 1.0.0
5. The device turns off when the user **Format Card** in BioStar 2. Affects version: 1.0.0

Firmware Version 1.7.1 (Build No. 1.7.1_20230502_210200_tw)

Release | 2023-06-08

Hanwha Techwin OEM FW

Bug Fixes

1. Only Hanwha Techwin SDK is allowed to connect. (Except BS2_GetFactoryConfig)
2. The firmware upgrade is available only with Hanwha Techwin OEM firmware.
3. Remove all relay action.

Firmware Version 1.7.1 (Build No. 1.7.1_221220)

Release | 2023-01-11

> **Caution**
> Devices with the new SE processor cannot downgrade to a lower version after upgrading the firmware to v1.7.1 or later. 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.

New Features and Improvements

1. Supports a new SE processor and new firmware.
2. Separated the log related to the cause of the door unlock.
    - Door open request by exit button
    - Door open request by operator
3. 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.

Bug Fixes

1. Card types not checked to be used in smart card settings gets issued normally Affects version: 1.5.0.
2. Improved the structure to prevent authentication fail caused by broken database or cache memory Affects version: 1.0.0.

Firmware Version 1.7.0 (Build No. 1.7.0_220509)

Release | 2022-06-16

> **Caution**
> Devices with the new SE processor cannot downgrade to a lower version after upgrading the firmware to v1.7.0 or later. 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.

New Features and Improvements

1. Supports setting the byte order for smart cards.
   - Supports setting the byte order of data to be output to Wiegand or OSDP.
2. Improved the Arm/Disarm status is maintained if the device loses power.
3. Supports the dual SE processor.

Bug Fixes

1. Mobile card authentication suddenly does not work Affects version: 1.0.0.
2. The device failed to recognize the iCLASS Seos card intermittently before rebooting the device (BEW2-OAP, BEW2-OAPB) Affects version: 1.0.0.
3. 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: 1.6.3.
4. Incorrect Bit Count and card data were output when the device was connected to a 3rd-party system via OSDP and the CSN card was registered in Wiegand format and authenticated Affects version: 1.6.3.
5. 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: 1.0.0.
6. 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: 1.6.3.
7. Device does not recognize certain HID iCLASS Seos cards Affects version: 1.0.0.

Firmware Version 1.6.3 (Build No. 1.6.3_210419)

Release | 2021-04-20

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. Improved that LFD Driver IC damage does not affect fingerprint recognition performance.
4. The transmission power level for Bluetooth Low Energy (BLE) has been adjusted.

Bug Fixes

1. Card data were output with the wrong BitCount when the device was connected to a 3rd-party system via OSDP. Affects version: 1.0.0
2. When calling the BS2_ResetConfigExceptNetInfo API from the BioStar Device SDK, a 'Timeout' error occurred. Affects version: 1.0.0
3. 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 1.5.0 or later) Affects version: 1.0.0
4. 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: 1.0.0
5. After initializing the slave device's settings, it was not able to connect it to a 3rd-party controller. Affects version: 1.6.0

Firmware Version 1.6.2 (Build No. 1.6.2_201202)

Release | 2020-12-02

Bug Fixes

1. After the firmware of both a master device and a slave device was upgraded to the version 1.6.x., the reconnection between devices failed when rebooting the slave device. (BEW2-OAP, BEW2-OHP, BEW2-ODP)
2. Delay occurred intermittently when reading a FeliCa card. (BEW2-OAPB, BEW2-OHPB, BEW2-ODPB)

Firmware Version 1.6.1 (Build No. 1.6.1_201113)

Release | 2020-11-13

Bug Fixes

1. Device shows low reading performance. (BEW2-OAPB)

Firmware Version 1.6.0 (Build No. 1.6.0_200902)

Release | 2020-09-10

New Features and Improvements

1. Supports Secure Boot.
    - BEW2-OAPB, BEW2-OHPB, BEW2-ODPB
2. Supports Mobile Access.
    - BEW2-OAP, BEW2-OHP, BEW2-ODP: NFC
    - BEW2-OAPB, BEW2-OHPB, BEW2-ODPB: BLE, NFC
3. Separated event logs of Mobile Access cards and RFID cards.

Bug Fixes

1. iCLASS card does not get read as a Wiegand card unless the iCLASS was also selected on the Smart Card mask.
2. Device responded that it supports transparent mode by OSDP_PDCAP when connecting as slave while it does not support it.
3. When using a static IP while DNS server address is configured, a reboot on the device causes communication problems between the server.
4. Incorrect BitCount is sent if a user authenticates with AoC when the device is connected to a 3rd-party system via OSDP.
5. If 31 slave devices are connected and one of the devices get disconnected, the master device will reboot.

Firmware Version 1.5.0 (Build No. 1.5.0_200722)

Release | 2020-07-29

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. Improved the device to recognize unknown cards by selecting the card type options. (BEW2-OAP)
2. OSDP Communication does not work normally if the value sent to the slave device is greater than the defined value.
3. Device reboots or a timeout occurs when upgrading firmware or transferring user data during SSL secure communication.
4. The event log of the device is not sent in the order in which it occurred.
5. Issue that the option for card types is deactivated when the device is connected as a slave after the factory reset.
6. Issue that the connection of the slave device is disconnected when the slave device is connected.
7. Device reboots when there is no operation after connecting power.
8. Device shows low reading performance with low frequency cards even when card is placed within an operating distance.

Firmware Version 1.4.1 (Build No. 1.4.1_190911)

Release | 2019-09-18

Bug Fixes

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

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. 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.
5. Increase of the number of administrators that can be added.
6. Increase of the maximum number of floor levels.
7. Supports options for selection by card type.
8. Support to the Clear APB for each user.
9. Supports checking module firmware version.
10. Supports the latest version of I/O module Micom (V1.3.1).
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. The output such as LED status indicator or buzzer is not supported for authentication failure due to Live Finger Detection (LFD).
3. It does not respond to inputs from the slave device when booting the master device.
4. Applies FA improvement algorithm.
5. Start time is not applied in UTC when importing filtered logs using SDK.
6. A user cannot access BioStar 1.93 when using the latest firmware.
7. The device cannot recognize iCLASS cards issued by the first generation device.
8. Supports unsupported devices (FaceStation 2, FaceLite).
9. HID Prox cards are continously recognized.
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)
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

Bug Fixes

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

Main Fixes

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

New Features and Improvements

1. Improves the data protection.
    - Increase the items to encrypt the data.
    - Support to setting the period for storing the personal information.
2. Change the maximum value of the interval and width for the Wiegand Input.
3. Support to the number of users, fingerprints, faces, and cards in Manage Users in Device.
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 DESFire/DESFire V1 Advanced option.
9. Support to AES encryption type for DESFire card.
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 1.2.3 (Build No. 1.2.3_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 1.2.2 (Build No. 1.2.2_180710)

Release | 2018-07-24

Bug Fixes

1. The device restarts when authentication fails.
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

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

Bug Fixes

1. Problem that is affected by the schedule set on the device, even though the smart card is set to the bypass card.
2. Issue where the bypass does not work when authentication with AoC in Wiegand output.
3. Issue where event logs and real-time logs are not uploaded normally to BioStar 2.
4. Problem that relay state is not maintained when reconnecting a device connected by RS-485.
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.
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.
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.
8. Problem that does not respond to the input ground.
9. Modified to limit kernel downgrade based on the hardware version of the device.
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

New Features and Improvements

1. Output signal setting for Wiegand reader control.
2. Improves that invalid values can not be entered in the authentication mode, AuthTimeout, MsgTimeout, ScanTimeout, and MatchingTimeout.
3. Support fingerprint enrollment on slave device.
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.
5. Performs the Access on Card (AoC) matching when connected to a master device as a slave device.
6. Support SEOS smart cards (Elite Key).
7. Improves performance of SEOS smart card RF reading.
8. Improves user transfer speed.
9. Improves log search within device.
10. User Operator cannot change another user's Operator Level as Administrator.
11. Support Reset without Network Settings.
12. Support Daylight Saving Time setting.
13. Improves Trigger & Action for duress finger.
14. Support Private Authentication on AoC.
15. Improves to handle the encryption key of the important information stored in database differently from server to server.
16. Support One Device Mode(Legacy).
17. Added a message asking whether to delete the fingerprint in the database after completing AoC issuance.
18. Support the secure tamper.
19. Support ISO14443A 10 Byte CSN.
20. Support connecting with BioEntry R2, BioEntry P2, BioLite N2, XPass D2.

Bug Fixes

1. Problem trying to forward commands related to Config during connection after searching RS-485 slave device.
2. Problem not working in 256 bit Wiegand format.
3. Problem with reading mobile smart cards on Galaxy S4.
4. Galaxy S5 NFC is recognized as a CSN card when authenticating with NFC and the authentication fails.
5. Issue where the device can not read HID Prox II card.
6. Issue where the fingerprint sensor does not work.
7. Fixed that Hard APB authentication failure notification is distinguished from general authentication failure notification.
8. Problem that the user ID type in the slave device can not be set in alphanumeric characters.
9. Issue that does not work when template size is set to 384 bytes when issuing NFC card.
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

New Features and Improvements

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

New Features and Improvements

1. Improved Live Finger Detection(LFD) performance

Bug Fixes

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

New Features and Improvements

1. Support 8GB eMMC.
2. Performs the validation when invalid values are sent to the device.
3. Support SEOS smart cards.

Bug Fixes

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

New Features and Improvements

1. Add Lift I/O MFG Command

Bug Fixes

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

Firmware Version 1.1.1 (Build No. 1.1.1_161213)

Release | 2016-12-20

Bug Fixes

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

New Features and Improvements

1. Support for the secure communication (TLS) with BioStar 2
2. Support for iCLASS SEOS card
3. Support for the 1.x Template on Card
4. Support for the daylight saving time
5. OP6 sensor support
6. Improved fingerprint algorithm
7. Improved LFD calibration
8. Support for alphanumeric ID
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

Bug Fixes

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

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

© 2026 Suprema Inc. Suprema and identifying product names and numbers herein are registered trade marks of Suprema, Inc.
All non-Suprema brands and product names are trademarks or registered trademarks of their respective companies.
Product appearance, build status and/or specifications are subject to change without notice.